Πανεπιστήμιο Πειραιώς
University of Piraeus

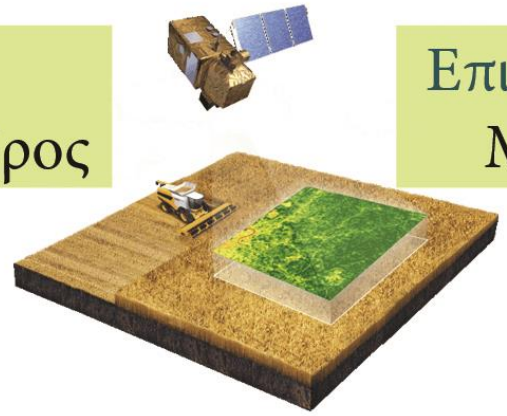
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Κλιματική Κρίση και Τεχνολογίες Πληροφορικής και Επικοινωνιών

Διπλωματική Εργασία

Η Κυβερνοασφάλεια στους τομείς της Κλιματικής Κρίσης

Έρευνα:
Ιακωβάκης Αλέξανδρος

Επιβλέπων Καθηγητής:
Μανιάτης Ιωάννης



Πειραιάς 2023

Δήλωση Πνευματικών Δικαιωμάτων

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο:

«Η Κυβερνοασφάλεια στους τομείς της Κλιματικής Κρίσης»

καθώς και τα ηλεκτρονικά αρχεία και οι πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν και η οποία έχει εκπονηθεί στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή:
Α.Ιακωβάκης

Ευχαριστίες

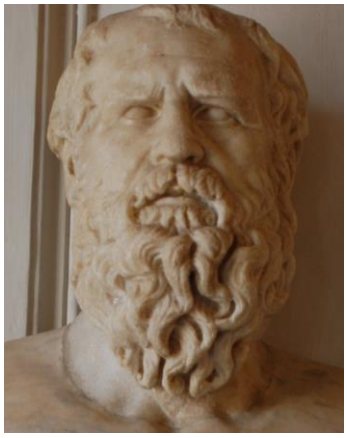
Η παρούσα διπλωματική εργασία πραγματοποιήθηκε στο Πανεπιστήμιο Πειραιώς στο τμήμα Ψηφιακών Συστημάτων στο πλαίσιο του Προγράμματος Μεταπτυχιακών Σπουδών: «Κλιματική Κρίση και Τεχνολογίες Πληροφορικής και Επικοινωνιών», κατά το έτος 2023.

Ευχαριστώ εκ βαθέων όλους τους συντελεστές του παρόντος μεταπτυχιακού προγράμματος. Αρχίζοντας από τον καθηγητή μου κύριο Ιωάννη Μανιάτη για την ενεργειακή σοφία αλλά και την καθοδήγηση που μας παρείχε καθ'όλη τη διάρκεια της φοίτησης, τον κύριο Θάνο Δογάνη για τη διάθεση, την ενασχόληση και τις γνώσεις που μας μεταλαμπάδευσε στον τομέα των G.I.S., τον κύριο Μόσχο Κορασίδη για την καθοδήγηση στον τομέα της Γεωργίας Ακριβείας και της γεωπονίας, την κυρία Αμαλία Πολυδωροπούλου για τις γνώσεις που μας παρείχε στους τομείς της Συγκοινωνιολογίας και των Μεταφορών και Αποθήκευσης προϊόντων και τέλος, την Ιωάννα Βούλγαρη για την άμεση ανταπόκρισή της όσον αφορά την οργάνωση της δομής και λειτουργίας του Π.Μ.Σ.

Ευχαριστώ συν τοις άλλοις τον κύριο Αναστάσιο Βουδούρη για την επικοινωνία και θετική ανταπόκρισή του καθ'όλη τη διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας και τον κύριο Χρήστο Ξενάκη που κατά τη διάλεξή του για τη Κυβερνοασφάλεια στα Smart Grids μου ενεργοποίησε το ερευνητικό ενδιαφέρον και με ενέπνευσε ώστε να ακολουθήσω την εξέταση της Κυβερνοασφάλειας και τον ρόλο των νέων τεχνολογιών και στους υπόλοιπους τομείς που έχουν κομβικό ρόλο στην αντιμετώπιση της Κλιματικής Κρίσης, πέραν των τομέων της Ενέργειας και των Έξυπνων Πόλεων που αφορούσε η εν λόγω διάλεξη.

Τέλος, ευχαριστώ τους συμφοιτητές που συντονιστήκαμε κατά την εκπόνηση των εργασιών του παρόντος Π.Μ.Σ., αλλά και την οικογένεια, τις φίλες και τους φίλους μου για την αμέριστη συμπαράστασή τους.

Ἐὰν μὴ ἔλπηαι, ἀνέλπιστον οὐκ ἐξευρήσει, ἀνεξερεύνητον ἐὸν καὶ ἄπορον.[1]
Ἡράκλειτος ὁ Ἐφέσιος, 6ος – 5ος αιώνας π.Χ.



Εάν δεν ελπίζεις στο ανέλπιστο, δεν θα το βρεις!

[1] Πηγή: https://www.loebclassics.com/view/heracleitus_philospher-universe/1931/pb_LCL150.473.xml

Περιεχόμενα

Περίληψη

Το φαινόμενο του θερμοκηπίου είναι το κύριο αίτιο της κλιματικής κρίσης. Ορισμένα αέρια, με κυριότερα το μεθάνιο, το διοξείδιο του άνθρακα, τα φθοριούχα αέρια και το οξείδιο του αζώτου στην ατμόσφαιρα της Γης μιμούνται την επίδραση του γυαλιού του θερμοκηπίου παγιδεύοντας την ηλιακή θερμότητα και εμποδίζοντάς την να διαφύγει πίσω στο διάστημα, γεγονός το οποίο συμβάλλει στην υπερθέρμανση του πλανήτη και στην αύξηση των ξαφνικών καιρικών αλλαγών και σε διαρκώς αυξανόμενης έντασης επικίνδυνων καιρικών φαινομένων. Χαρακτηριστικά, η ατμοσφαιρική συγκέντρωσή του διοξειδίου του άνθρακα αυξήθηκε στο 48% σε σχέση με τα προβιομηχανικά επίπεδα (πριν από το 1750) μέχρι το 2020.[2]

Στην Ευρωπαϊκή Ένωση, το δεύτερο τρίμηνο του 2022, οι τομείς της οικονομίας οι οποίοι εξέπεμψαν τις περισσότερες εκπομπές αερίων του θερμοκηπίου ήταν οι Κατασκευές και η Μεταποίηση (23%), η Ηλεκτρική Ενέργεια, η παροχή Αερίου (19%) και τα Νοικοκυριά (17%), ακολουθούμενες από τις Μεταφορές και την Αποθήκευση Προϊόντων (14%) και τη Γεωργία (13%).[3]

Ο ρόλος της Πληροφορικής και των Τεχνολογιών των Επικοινωνιών αναδεικνύεται κομβικός εφόσον οδηγεί τόσο στην ψηφιοποίηση των διαδικασιών, όσο και στην ολοένα αποδοτικότερη χρήση των πόρων στους προαναφερθέντες τομείς. Ωστόσο, προϋπόθεση για την ομαλή λειτουργία των πληροφοριακών συστημάτων και των τηλεπικοινωνιών είναι η τήρηση και η λήψη μέτρων ασφαλείας, δηλαδή η Κυβερνοασφάλεια. Πιο συγκεκριμένα, το ζητούμενο στην Κυβερνοασφάλεια, είναι η ασφάλεια των συσκευών και των δεδομένων από επιθέσεις πολλών πλευρών που έχουν στόχο την καταστροφή ή την αλίευση δεδομένων.

Σκοπός της διπλωματικής εργασίας είναι η μελέτη της Κυβερνοασφάλειας και η ανάδειξη της σημασίας της στους βασικούς τομείς που συντελούν στην Κλιματική Κρίση, στην Ευφυή Γεωργία, στις Μεταφορές και την Αποθήκευση Προϊόντων (Logistics) και τέλος στην Ενέργεια και στις Έξυπνες Πόλεις του μέλλοντος. Η έρευνα πραγματοποιήθηκε τόσο χρησιμοποιώντας βιβλιογραφία από επιστημονικά άρθρα εφαρμόζοντας τις κατάλληλες βιβλιομετρικές μεθόδους, όσο και αξιοποιώντας στοιχεία διαπιστευμένων πηγών, δηλαδή έρευνες και ειδησεογραφία από το διαδίκτυο.

Στο πρώτο κεφάλαιο παρουσιάζεται και αναπτύσσεται η σημασία της Κυβερνοασφάλειας στη Γεωργία Ακριβείας. Στο δεύτερο κεφάλαιο αναλύεται η τεχνολογία Blockchain, ήτοι του πρωτοκόλλου του μέλλοντος στην Κυβερνοασφάλεια, στον χώρο των Μεταφορών και Αποθήκευσης Προϊόντων. Τέλος, στο τρίτο κεφάλαιο όσον αφορά τους χώρους της Ενέργειας και των Έξυπνων Πόλεων, πραγματοποιείται έρευνα στα επερχόμενα Έξυπνα Δίκτυα Ηλεκτρικής Ενέργειας και τους κανόνες Κυβερνοασφάλειας που θα τα διέπουν.

[2] Πηγή: https://climate.ec.europa.eu/climate-change/causes-climate-change_en

[3] Πηγή: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Quarterly_greenhouse_gas_emissions_in_the_EU#Greenhouse_gas_emissions

Abstract

The greenhouse effect is the main cause of the climate crisis. Certain gases, notably methane, carbon dioxide, fluorine gases and nitrous oxide, in the Earth's atmosphere mimic the impact of glass in a greenhouse, by trapping solar heat and preventing it from escaping back into space, contributing to global warming and consequently driving into the increase in sudden weather changes and ever-increasing intensity of dangerous weather events. Moreover, the atmospheric concentration of carbon dioxide increased at about 48% of pre-industrial levels (before 1750) by 2020.

In the European Union, in the second quarter of 2022, the sectors of economy which emitted the most greenhouse gases were Construction and Manufacturing (23%), Electricity and Gas Supply (19%) and Households (17%), followed by product Transport and Storage, also known as Logistics, (14%) and Agriculture (13%).

The role of Information Technology and Communication Technologies emerges as crucial since it leads both to the digitization of processes and to the increasingly efficient use of resources in the above-mentioned areas. However, a prerequisite for the smooth operation of information systems and telecommunications is the observance and adoption of security measures, i.e. Cybersecurity. More specifically, what is required in Cybersecurity is the security of devices and data from attacks from many sides that aim to destroy or capture data.

The purpose of the thesis is the study of Cybersecurity and the highlighting of its' importance in the key sectors that contribute to the Climate Crisis, Precision Agriculture, Transport and Storage (Logistics) and finally the field of Energy and the Smart Cities of the future. The research was carried out using the bibliography from scientific articles while applying the appropriate bibliometric methods and using data from accredited sources, i.e. surveys and news from the Internet.

The first chapter presents and develops the importance of Cybersecurity in Precision Agriculture. The second chapter analyzes the Blockchain technology, i.e. the protocol of the future in Cybersecurity, in the area of Product Transportation and Storage. Finally, in the third chapter regarding the areas of Energy and Smart Cities, research is carried out on the upcoming Smart Grids of Electricity and the Cybersecurity rules that will govern them.

Πανεπιστήμιο Πειραιώς
University of Piraeus

Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Κλιματική Κρίση και Τεχνολογίες Πληροφορικής και Επικοινωνιών

Κεφάλαιο 1

Η Σημασία της Κυβερνοασφάλειας στην Γεωργία Ακριβείας

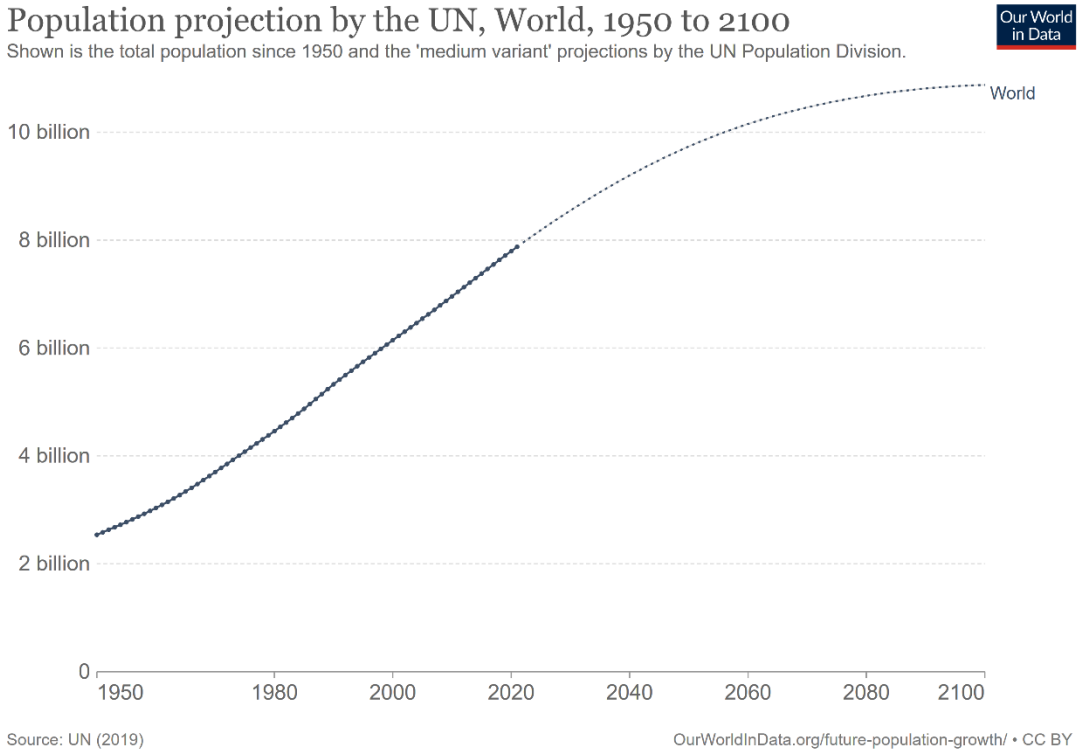
Πειραιάς
2023

1.1 Εισαγωγή 1ου κεφαλαίου

Ο πλανήτης μας σήμερα βρίσκεται αντιμέτωπος με μια άνευ προηγουμένου υπερεκμετάλλευση όλων σχεδόν των διαθέσιμων πόρων του. Η γενεσιουργός αιτία είναι καθαρά ανθρωπογενής και δημιουργεί υπαρκτούς κινδύνους επιβίωσης στο άμεσο μέλλον και για τον ίδιο τον άνθρωπό αλλά και για τα υπόλοιπα είδη με τα οποία μοιράζεται τον πλανήτη.

Η υπερεκμετάλλευση των πόρων του πλανήτη μας δεν είναι μόνο αποτέλεσμα ενός συστήματος ανάπτυξης που βασίζεται στον υπερκαταναλωτισμό, αλλά και σε ένα πολύ σημαντικό γεγονός, τον υπερπληθυσμό.

Εικόνα 1: Πληθυσμιακή προβολή από το 1950 έως το 2100



Πηγή: https://ourworldindata.org/grapher/UN-population-projection-medium-variant

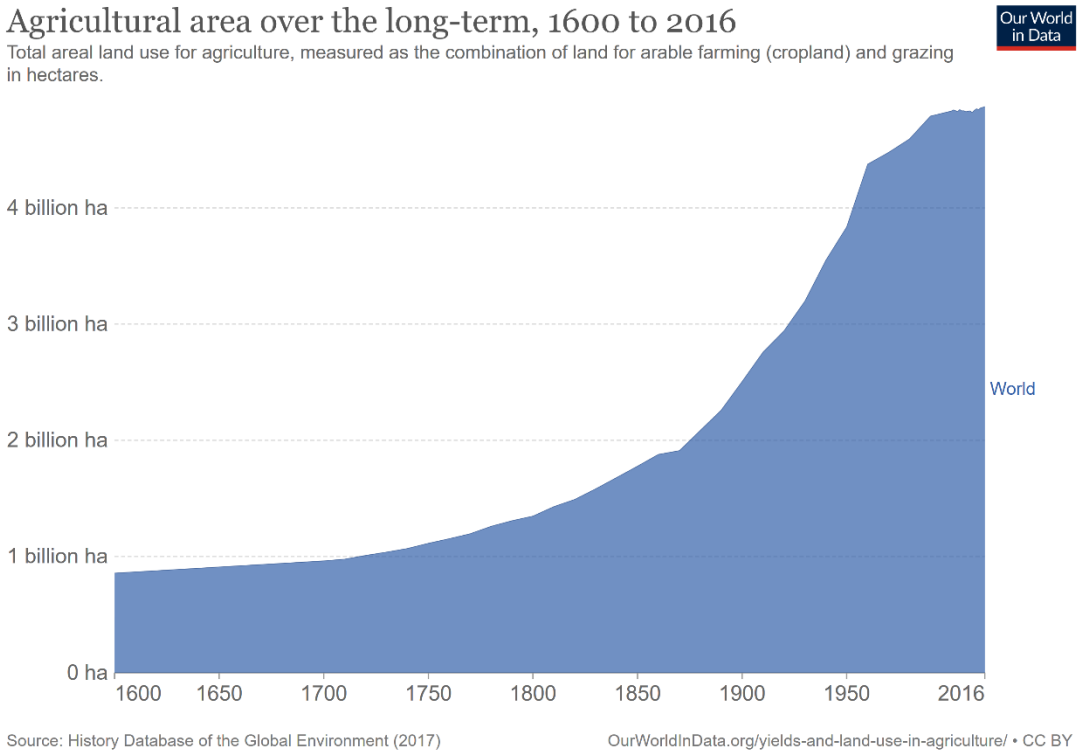
Ο ανθρώπινος πληθυσμός έφτασε το 1 δις στις αρχές του 1800, πιο συγκεκριμένα το 1804. Χρειάστηκαν δεκάδες χιλιάδες χρόνια προκειμένου ο πληθυσμός του είδους μας να φτάσει το 1 δις, ωστόσο απαιτήθηκαν μόλις σχεδόν 200 χρόνια για να φτάσουμε τα σχεδόν 7.8 δις σήμερα. Οι προβλέψεις[4] κάνουν λόγο για σχεδόν 11 δις μέχρι το τέλος του αιώνα μας.

[4] Πηγή: Max Roser, "Future Population Growth," *Our World in Data*, May 9, 2013, https://ourworldindata.org/future-population-growth.

1.2 Η σημασία της Γεωργίας Ακριβείας

Παρότι ο ανθρώπινος πληθυσμός αυξάνεται και σύμφωνα με τις παραπάνω εκτιμήσεις αναμένεται να αυξηθεί περαιτέρω, εντούτοις οι εκτάσεις γης για καλλιέργειες παραμένουν στάσιμες από τις αρχές του 2000, όπως φαίνεται και στο παρακάτω διάγραμμα[5].

Εικόνα 2: Γεωργικές εκτάσεις σε βάθος χρόνου, από το 1600 έως το 2016



Πηγή: https://ourworldindata.org/grapher/total-agricultural-area-over-the-long-term?country=~OWID_WRL

Η κλιματική κρίση, η έντονη αστικοποίηση καθώς και τελευταία η ανάγκη για την εύρεση χώρων για την εγκατάσταση ανανεώσιμων πηγών ενέργειας, αφαιρούν από τον αγροτικό τομέα τη δυνατότητα χρήσης επιπλέον γης. Πέραν των παραπάνω, ένας από τους πιο σημαντικούς πόρους του πλανήτη μας, το νερό, θα πρέπει και αυτός να χρησιμοποιείται με βάση έναν κανόνα: δεν είναι ανεξάντλητος. Έχοντας τα παραπάνω στοιχεία υπόψη, καθίσταται σαφές ότι ο αγροτικός τομέας θα πρέπει να αυξήσει σημαντικά την παραγωγή τροφής πιθανώς στην ίδια ποσότητα εκτάσεων που κατέχει σήμερα, χωρίς σπατάλη νερού, προκειμένου να υποστηριχτεί η επιπλέον αύξηση του πληθυσμού. Από τα παραπάνω προκύπτει αβίαστα ότι ο αγροτικός τομέας αναμένεται να διαδραματίσει έναν ιδιαίτερα σημαίνοντα ρόλο στα επόμενα χρόνια. Προκειμένου να το πετύχει αυτό απαιτείται η χρήση σύγχρονων επιστημονικών μεθόδων και πολύ περισσότερων εργαλείων των τεχνολογιών πληροφορικής και τηλεπικοινωνιών.

[5] Πηγή: Hannah Ritchie and Max Roser, “Land Use,” *Our World in Data*, November 13, 2013, https://ourworldindata.org/land-use.

1.3 Εννοιολογική Προσέγγιση

Η Γεωργία Ακριβείας (PA, Precision Agriculture) αφορά τη διαχείριση της γεωργίας που βασίζεται στην παρατήρηση, στην λήψη μετρήσεων και στην στοχευμένη απόκριση η οποία μπορεί να τροποποιήσειτις εισροές σε κάθε σημείο του αγρού βασιζόμενη στις μεταβαλλόμενες και πραγματικές ανάγκες της καλλιέργειας[6]. Λόγου χάρη, στην ίδια καλλιέργεια διαφορετικά σημεία του αγρού έχουν διαφορετικές ανάγκες όσον αφορά το νερό για ποικίλους λόγους. Με τα τεχνολογικά εργαλεία που του παρέχει η Γεωργία Ακριβείας, ο αγρότης μπορεί να μετρήσει αυτή τη διαφορετικότητα όσον αφορά την ανάγκη σε νερό και να επέμβει δυναμικά τροποποιώντας ανάλογα τις εισροές νερού. Το ίδιο ακριβώς μπορεί να γίνει και με τα λιπάσματα όπως και με τα ζιζανιοκτόνα. Η έρευνα για εφαρμογές της Γεωργίας Ακριβείας ξεκίνησε περίπου στα μέσα της δεκαετίας του 1980. Παραταύτα, μόνο από τα μέσα της δεκαετίας του 1990 άρχισαν να εμφανίζονται σιγά σιγά πρακτικές εφαρμογές της Γεωργίας Ακριβείας με αισθητήρες που μετρούσαν την αγωγιμότητα του εδάφους, την υγρασία του και την περιεκτικότητα χλωροφύλλης στην καλλιέργεια.

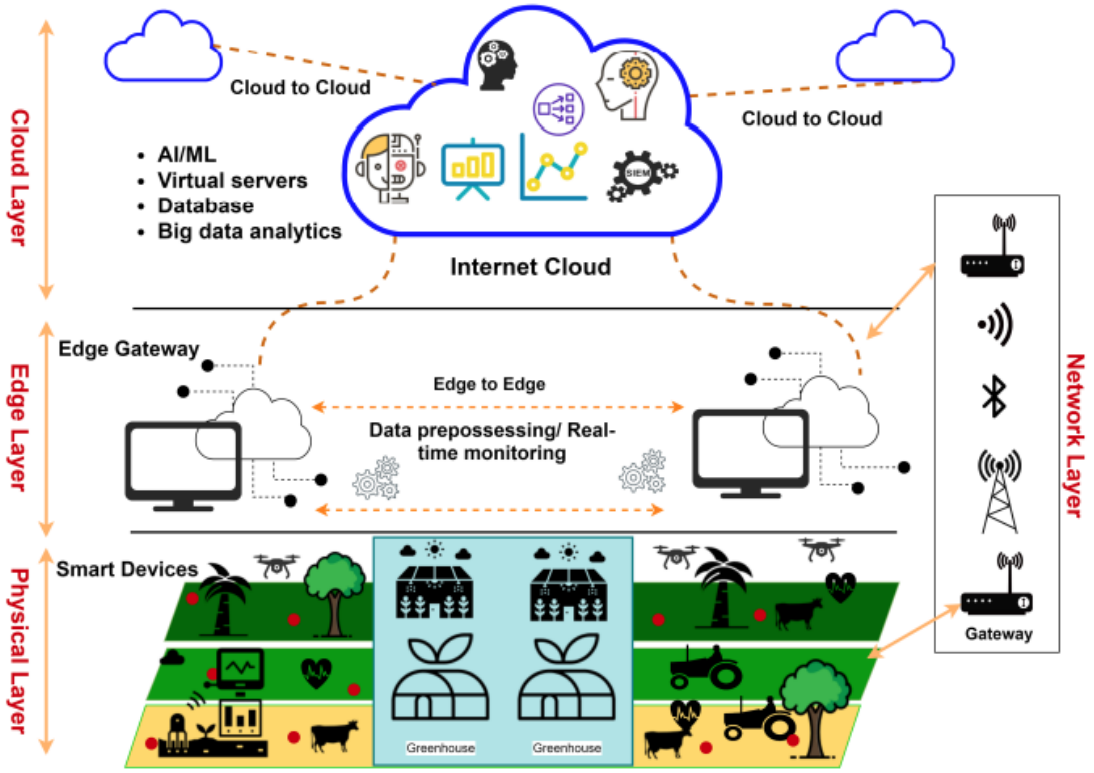
Ωστόσο, η πραγματική επανάσταση στη γεωργία ακριβείας ξεκίνησε ουσιαστικά από το 2015. Τότε άρχισαν να κάνουν την εμφάνισή τους τα λεγόμενα farmbots, δηλαδή, αυτόνομα συστήματα άρδευσης και ψεκασμού. Η ραγδαία όμως ανάπτυξη των τεχνολογιών IoT (Internet of Things) ήταν αυτή που έδωσε μια πραγματική ώθηση στην εξάπλωση της ιδέας της Γεωργίας Ακριβείας και στην εφαρμογή της στον αγρό. Η εμφάνιση φθηνών και εξελιγμένων αισθητήρων οι οποίοι άρχισαν να υιοθετούν τεχνολογία δικτύωσης LP – WAN (Low Power Wide Area Network), όπως τα LoRa WAN (2015) και Sigfox (2010)[7]. Συνεπώς, η Γεωργία Ακριβείας είναι άρρηκτα συνδεδεμένη με την εφαρμογή των τεχνολογιών πληροφορικής και επικοινωνιών και ειδικότερα του IoT στο τομέα της γεωργίας. Η εφαρμογή αυτών των τεχνολογιών οδηγεί τη γεωργία στη λεγόμενη τρίτη Πράσινη Επανάσταση, η οποία βασίζεται ιδιαίτερα στην εφαρμογή αυτών των τεχνολογικών λύσεων, δηλαδή, το IoT, τους ενεργοποιητές και αισθητήρες, τα μη επανδρωμένα οχήματα, τα συστήματα γεωπληροφορικής, τα Big Data, και τη ρομποτική για την υλοποίηση των farmbots. Στον ελληνικό χώρο, η πρώτη εφαρμογή γεωργίας ακριβείας θεωρείται το Gaiasense[8].

Στην βιβλιογραφική έρευνα εντοπίστηκαν και άλλοι βασικοί όροι που περιγράφουν ή και πλησιάζουν πολύ την έννοια της Γεωργίας Ακριβείας και χρησιμοποιούνται εναλλακτικά. Ο δεύτερος πιο συχνά χρησιμοποιούμενος είναι η Έξυπνη Γεωργία (Smart Farming). Επιπροσθέτως, μια εννοιολογική διευκρίνηση είναι απαραίτητο να γίνει σε αυτήν την περίπτωση. Η Γεωργία Ακριβείας εφαρμόζει τεχνολογίες IoT, οι οποίες παρέχουν τη δυνατότητα ελέγχου και τροποποίησης των εισροών με ιδιαίτερα μεγάλη ακρίβεια. Επιπλέον, υποβοηθάται στη λήψη αποφάσεων από ολοκληρωμένα πληροφοριακά συστήματα που τρέχουν ως υπηρεσία στο Υπολογιστικό Νέφος (Cloud). Τέλος, έχει να κάνει με την αυτοματοποιημένη αντίδραση του ολοκληρωμένου πληροφοριακού συστήματος της Γεωργίας Ακριβείας να δώσει στον αγρότη πιθανές λύσεις όταν παρουσιαστεί μια μεταβολή σε μια από τις

[6] Πηγή: “Precision Agriculture,” στη *Wikipedia*, Ανακτήθηκε την 1 Ιουλίου 2022, https://en.wikipedia.org/w/index.php?title=Precision_agriculture&oldid=1095898381.
[7] Πηγή: “Low-Power Wide-Area Network,” στη *Wikipedia*, Ανακτήθηκε στις 16 Μαρτίου 2022, https://en.wikipedia.org/w/index.php?title=Low-power_wide-area_network&oldid=1077542034.
[8] Πηγή: “Γίνετε πρωτοπόροι της ευφυούς γεωργίας στην Ελλάδα | gaiasense,” *gaiasense - Ευφυής γεωργία* (blog), Ανακτήθηκε στις 18 Ιουλίου 2022, https://www.gaiasense.gr/gaiasense.

μεταβλητές που παρακολουθεί (θερμοκρασία, υγρασία, ηλεκτρική αγωγιμότητα του εδάφους κτλ.).

Εικόνα 3: Αρχιτεκτονική Ακριβούς Γεωργίας



Πηγή: https://www.researchgate.net/publication/353947996_A_Review_on_Security_of_Smart_Farming_and_Precision_Agriculture_Security_Aspects_Attacks_Threats_and_Countermeasures

Στο παραπάνω στιγμιότυπο έχουμε μια τυπική πολυεπίπεδη αρχιτεκτονική ενός συστήματος ακριβούς γεωργίας. Όπως αποτυπώνεται και στην εικόνα οι τεχνολογίες πληροφορικής, επικοινωνιών και IoT είναι παρούσες σε κάθε επίπεδο. Με τόσο μεγάλη ολοκλήρωση και εξάρτηση της Γεωργίας Ακριβείας, σχεδόν σε κάθε επίπεδο από τις τεχνολογίες πληροφορικής και επικοινωνιών, είναι επόμενο να τίθενται ερωτήματα σχετικά με την ασφάλεια των συστημάτων, των διακινουμένων πληροφοριών και δεδομένων και κατ' επέκταση όλης της επιχείρησης ή του οργανισμού[9].

Τα πληροφοριακά συστήματα σε κάθε είδους οργανισμό, εταιρεία, επιχείρηση, μικρή, μεγάλη ή πολύ μεγάλη έχουν ένα κοινό χαρακτηριστικό, έναν κοινό παρανομαστή. Αποτελούν πολύπλοκες υπολογιστικές υποδομές οι οποίες βρίσκονται εκτεθειμένες στον κίνδυνο κυβερνοεπιθέσεων κάθε λεπτό της ημέρας. Είναι χαρακτηριστικό ότι σύμφωνα με τον Robert S. Mueller[10] υπάρχουν δυο ειδών εταιρείες στον κόσμο αυτές που έχουν ήδη δεχτεί κυβερνοεπίθεση και αυτές που θα

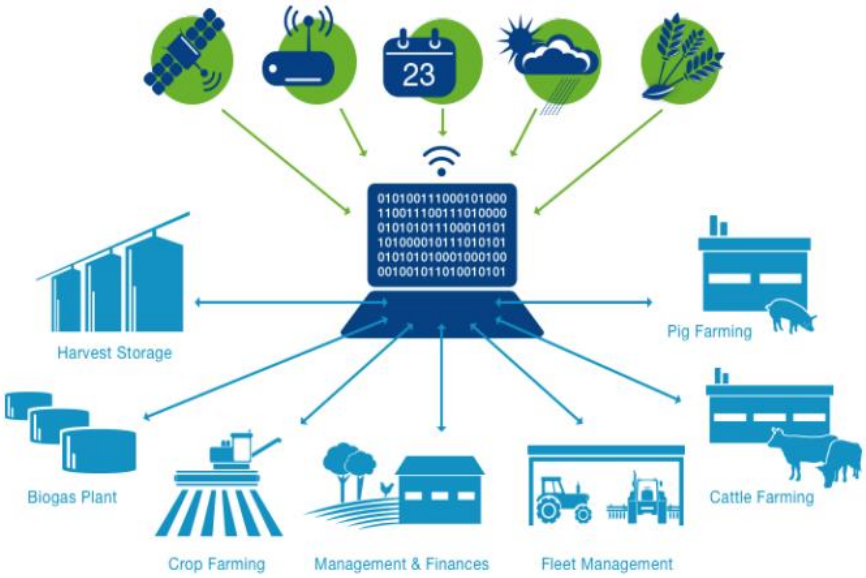
[9] Πηγή: Zsanett Angyalos, Szilvia Botos, and Szilagyi Robert, "The Importance of Cybersecurity in Modern Agriculture," *Journal of Agricultural Informatics* 12, Ανακτήθηκε στις 15 Ιουνίου 2022 https://doi.org/10.17700/jai.2021.12.2.604.

[10] Πηγή: "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies," FBI, Ανακτήθηκε στις 18 Ιουλίου 2022, https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

δεχτούν. Τελικά, καταλήγουν σε μια κατηγορία: Αυτές που δέχτηκαν κυβερνοεπίθεση και θα δεχτούν ξανά *«I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again».*

Σύμφωνα με τη CISCO[11] η κυβερνοασφάλεια αφορά μεθόδους και πρακτικές (best practices) για την προστασία συστημάτων, δικτύων, και προγραμμάτων από ψηφιακές απειλές. Οι κυβερνοεπιθέσεις έχουν συνηθέστερα ως στόχο την απόκτηση πρόσβασης σε πληφορορικά συστήματα και την αλίευση, αλλοίωση ή καταστροφή ευαίσθητων πληροφοριών. Επίσης, οι επιθέσεις αυτού του τύπου, πολύ συχνά αποσκοπούν στον εκβιασμό χρηστών για υποκλοπή χρηματικών ποσών ή για να προκαλέσουν πρόβλημα ή αναστάτωση ή ακόμα και διακοπή των καθημερινών διαδικασιών των επιχειρήσεων ή οργανισμών. Η εφαρμογή αποτελεσματικών μέτρων Κυβερνοασφάλειας αποτελεί μια πρόκληση σήμερα, διότι τα μηχανήματα που πρέπει να προστατέψουμε είναι διασυνδεδεμένα και πολύ περισσότερα σε αριθμό από τους ανθρώπους μέσα σε μια επιχείρηση ή έναν οργανισμό και επειδή οι επιτιθέμενοι γίνονται όλο και πιο εφευρετικοί και πιο πολυμήχανοι.

Εικόνα 4: Διασυνδεδεμένα Πληροφοριακά Συστήματα στη Γεωργία Ακριβείας



Πηγή: https://www.researchgate.net/profile/Szilagyi-Robert/publication/352412158/figure/fig2/AS:1035047431831553@1623785946482/Interconnected-Systems.png

1.4 Βιβλιομετρική Έρευνα

Στο παρόν κεφάλαιο διεξήχθη μια βιβλιομετρική έρευνα η οποία οδηγεί στην εξαγωγή συμπερασμάτων σχετικά με την υφιστάμενη ερευνητική δραστηριότητα στην κυβερνοασφάλεια και στη γεωργία ακριβείας, αλλά και στο σχηματισμό μίας σαφούς εικόνας για τις μελλοντικές τάσεις της έρευνας σε αυτό το θέμα.

Οι βιβλιομετρικές μέθοδοι χρησιμοποιούνται στην επιστήμη της Πληροφόρησης. Κάνουν χρήση κυρίως στατιστικών μεθόδων προκειμένου να αναλύσουν βιβλία, άρθρα και δημοσιεύσεις, αναφορικά με το επιστημονικό τους

[11] Πηγή: "What Is Cybersecurity?," Cisco, Ανακτήθηκε στις 18 Ιουλίου 2022, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

περιεχόμενο[12]. Μια ιδιαίτερα γνωστή μέθοδος βιβλιομετρίας είναι η ανάλυση των παραπομπών (citations). Με τη βοήθεια της ανάλυσης παραπομπών δύναται να κατασκευαστεί ένας γράφος, δηλαδή μια οπτική αναπαράσταση ενός δικτύου παραπομπών ανάμεσα σε δημοσιεύσεις. Με αυτόν τον τρόπο απεικονίζονται οι σχέσεις μεταξύ συγγραφέων, δημοσιεύσεων και όρων που χρησιμοποιούνται για να περιγράψουν θεματικές περιοχές ή ενότητες. Επιπλέον, παρουσιάζονται συσχετισμοί και βάσει αυτών εξάγονται λογικά συμπεράσματα, όπως ποιές είναι οι τάσεις της έρευνας στο παρόν ή πως δείχνουν ότι διαμορφώνονται στο μέλλον σε ένα συγκεκριμένο επιστημονικό θέμα.

Ένα από τα εργαλεία που υπάρχουν για βιβλιομετρικές έρευνες είναι και το VOSviewer[13]. Το VOSviewer είναι ένα πρόγραμμα το οποίο έχει τη δυνατότητα βιβλιομετρικών αναλύσεων. Αναλυτικότερα, δημιουργεί οπτικοποιημένους γράφους οι οποίοι αναπαριστούν δίκτυα βιβλιομετρικών δεδομένων. Τα δίκτυα αυτά δημιουργούνται από το συσχετισμό μεταξύ των παραπομπών που παραθέτουν οι συγγραφείς στις επιστημονικές του δημοσιεύσεις. Το VOSviewer έχει επαυξημένες δυνατότητες οι οποίες περιλαμβάνουν εξόρυξη κειμένου (text mining), καθώς και δημιουργία δικτύων με οπτικοποιημένους γράφους μετά από εξόρυξη των βασικών όρων μιας επιστημονικής δημοσίευσης.

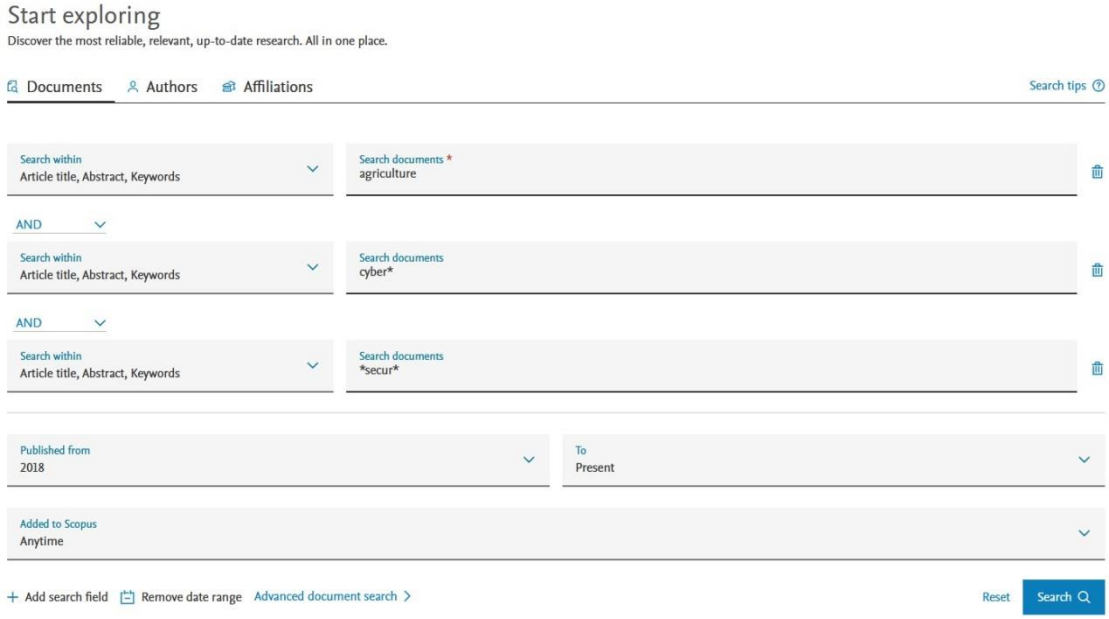
1.5 Μεθοδολογία και Εφαρμογή

Στην παρούσα έρευνα πραγματοποιήθηκε χρήση της επιστημονικής βάσης δημοσιεύσεων scopus.com. Πριν την κατάληξη στο ερώτημα με της σωστούς όρους αναζήτησης, δοκιμάστηκαν και ποικίλοι άλλοι όροι όπως οι: “smart farming”, “precision agriculture”, “cybersecurity”, “cyber” και “security”. Τελικά, το ερώτημα που περιείχε τη μέγιστη δυνατή ακρίβεια με το μέγιστοδυνατό πλήθος επιστρεφόμενων δημοσιεύσεων ήταν “agriculture”, “cyber*” και “*secur*”. Το ερώτημα αυτό φαίνεται ξεκάθαρα στο παρακάτω στιγμιότυπο.

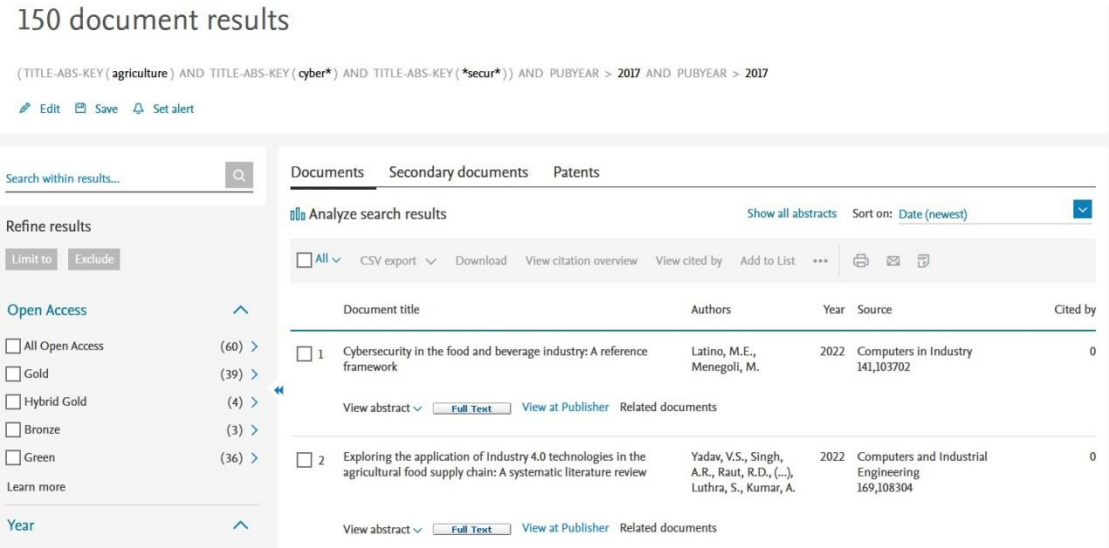
[12] Πηγή: “Bibliometrics,” in *Wikipedia*, Ανακτήθηκε στις 14 Ιουνίου 2022, https://en.wikipedia.org/w/index.php?title=Bibliometrics&oldid=1093153031.

[13] Πηγή: “VOSviewer - Visualizing Scientific Landscapes,” VOSviewer, Ανακτήθηκε στις 10 Ιουλίου 2022, https://www.vosviewer.com//.

Εικόνα 5: Στιγμιότυπο από τους όρους αναζήτησης στο scopus.com

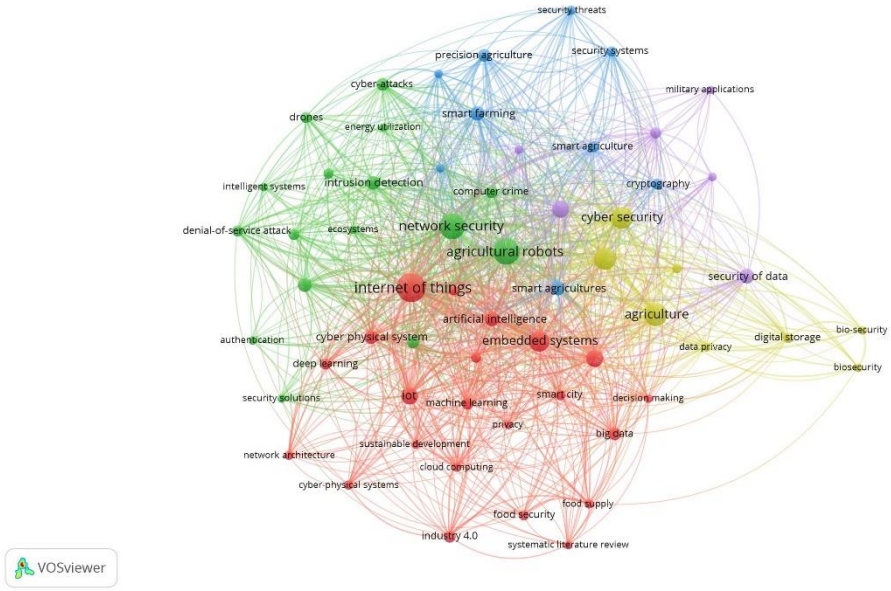


Εικόνα 6: Στιγμιότυπο από την επιστροφή των αποτελεσμάτων στο scopus.com

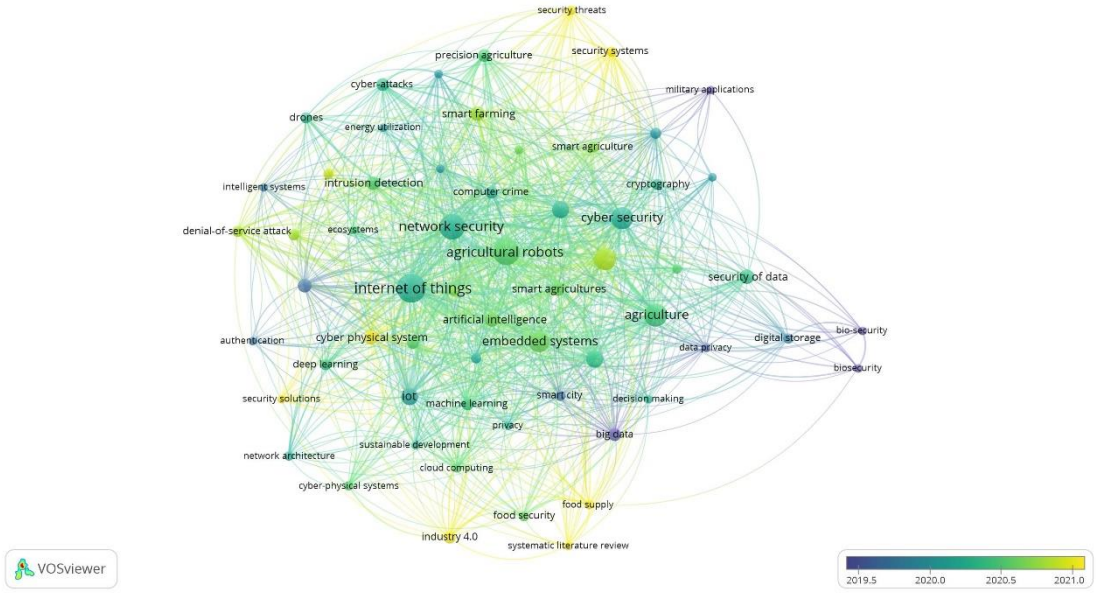


Τα επιστρεφόμενα αποτελέσματα έφτασαν τις 150 δημοσιεύσεις. Όσον αφορά τα χρονικά όρια των δημοσιευμένων έργων, κρίθηκε σκόπιμος ο περιορισμός της αναζήτησης μεταξύ του 2018 και του σήμερα. Τα εν λόγω αποτελέσματα εξήχθησαν σε ένα .csv αρχείο και εισήχθησαν στην εφαρμογή VOSviewer προκειμένου να οπτικοποιηθούν τα αποτελέσματα του δικτύου των βασικών όρων που εμφανίζονται στην επιστημονική βιβλιογραφία.

Εικόνα 7: Στιγμιότυπο από το Network Visualization της εφαρμογής VOSviewer



Εικόνα 8: Στιγμιότυπο από το Overlay Visualization της εφαρμογής VOSviewer



Τα παραπάνω στιγμιότυπα της παρουσιάζουν οπτικοποιημένα τα δίκτυα που σχηματίστηκαν από την εξαγωγή των βασικών όρων που υπάρχουν στην επιστημονική βιβλιογραφία και αφορούν τα ληφθέντα αποτελέσματα από την αναζήτηση στη βάση επιστημονικών δημοσιεύσεων scopus.com.

Στο πρώτο στιγμιότυπο της εφαρμογής VOSviewer, το οποίο ονομάζεται Network Visualization απεικονίζονται τα δίκτυα των βασικών όρων που έχει κατασκευάσει. Επειδή η Γεωργία Ακριβείας στην ουσία αποτελεί διεπιστημονικό αντικείμενο καθώς και πεδίο εφαρμογής των τεχνολογιών IoT, έχει ως αποτέλεσμα

ένα πολυσύνθετο και δαιδαλώδες δίκτυο πολλών βασικών όρων. Ωστόσο, τα παραπάνω στιγμιότυπα δυστυχώς είναι στατικά και δεν αναπαρίστανται οι πλήρεις δυνατότητες που παρέχει η ίδια η εφαρμογή VOSviewer. Πιο αναλυτικά, αν πάνω στο στον όρο «agriculture» παραμείνει για ελάχιστη ώρα ο δείκτης του ποντικιού, τότε η εφαρμογή θα «γκριζάρει» τους όρους που υπολείπονται πέραν του ιδίου όρου «agriculture» καθώς και τους βασικούς όρους με τους οποίους συνδέεται απευθείας. Όσο πιο έντονη και πιο μεγάλη σε μέγεθος είναι η εμφάνιση της γραμματοσειράς των βασικών όρων τόσο πιο πολλές φορές αυτοί εμφανίζονται στα δημοσιευμένα έργα και τόσο πιο ισχυρά δίκτυα έχουν με τους βασικούς όρους. Στην προκειμένη περίπτωση, ο όρος «agriculture robots» έχει προφανώς το μεγαλύτερο αριθμό εμφανίσεων και ακολουθείται από τους όρους «network security», «internet of things», «smart agricultures» κ.α. Αυτό που είναι αξιοσημείωτο εδώ, είναι ότι το VOSviewer αναδεικνύει τις τάσεις που διαμορφώνει η επιστημονική έρευνα την παρούσα στιγμή. Πιο συγκεκριμένα, διαχέεται η επιστημονική έρευνα όταν λόγου χάρη εξετάζουμε το θέμα της «smart agriculture» ή του «cybersecurity». Πέρα από αυτό, μπορούμε να δούμε και τη γειτνιάζουσα ερευνητική δραστηριότητα. Συγκεκριμένα, οι βασικοί όροι «data privacy» και «digital storage» συνδέονται μεταξύ τους, αλλά εμφανίζονται σε χαμηλότερη συχνότητα τόσο από το «cybersecurity» όσο και από το «agriculture».

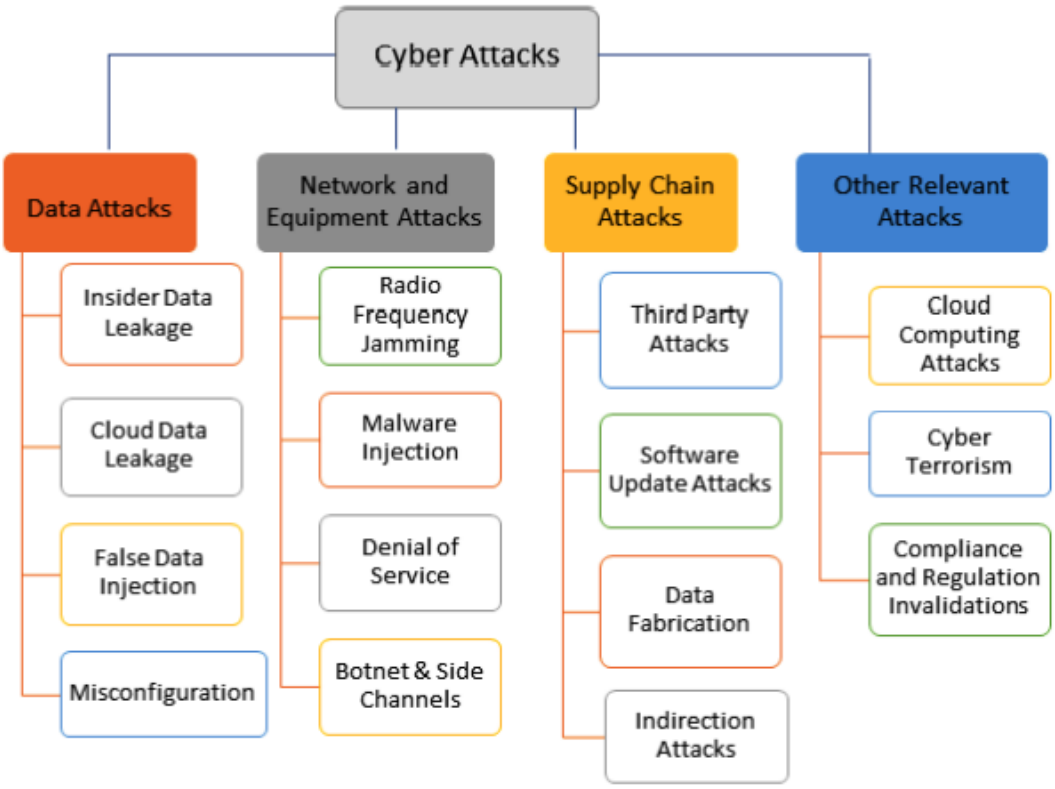
Το δεύτερο στιγμιότυπο της εφαρμογής VOSviewer ονομάζεται Overlay Visualization και παρέχει πληροφορίες όσον αφορά την ερευνητική δραστηριότητα στο πεδίο του χρόνου. Αναλυτικότερα, δίνονται απαντήσεις στο ποιές είναι οι μελλοντικές τάσεις της ερευνητικής δραστηριότητας στο συγκεκριμένο ερευνητικό πεδίο. Εξετάζοντας το δεύτερο στιγμιότυπο της εφαρμογής παρατηρείται ότι υπάρχει μια μικρή χρωματιστή μπάρα κάτω δεξιά. Αυτή η μπάρα αναπαριστά χρωματικά την ερευνητική δραστηριότητα σε βάθος χρόνου. Με κίτρινο απεικονίζονται οι βασικοί όροι οι οποίοι συγκεντρώνουν έντονη ερευνητική δραστηριότητα από τον Ιούνιο του 2020 και μετά. Αυτοί φαίνονται να είναι διασκορπισμένοι σε όλο σχεδόν το γράφο, γεγονός το οποίο υποδεικνύει ότι το αντικείμενο έρευνας της γεωργίας και της Κυβερνοασφάλειας είναι πολυσυλλεκτικό και ταυτόχρονα διεπιστημονικό. Συνεπώς, παρατηρείται πιο πρόσφατη δραστηριότητα για «security threats», «industry 4.0», «intrusion detection», «food supply», «smart farming» κ.α.

1.6 Ανατομία των Κυβερνοεπιθέσεων

Γενικότερα οι κυβερνοεπιθέσεις στον αγροτικό τομέα αναμένονται να προσομοιάζουν τις επιθέσεις στο χώρο της βιομηχανίας. Κυρίως, σε ό,τι αφορά τις μεθόδους, τις τακτικές και τους στόχους. Οι κυβερνοεπιθέσεις δε μοιάζουν πάντα μεταξύ τους, παρότι οι επιτιθέμενοι μπορεί να χρησιμοποιούν παρόμοιες τακτικές ή και τεχνολογίες. Επειδή στόχος των επιθέσεων στον γεωργικό τομέα είναι οι υπολογιστικές υποδομές, συμπεραίνουμε ότι η ανατομία των κυβερνοεπιθέσεων θα είναι αντίστοιχη με αυτή στο βιομηχανικό τομέα[14].

[14] Πηγή: Maanak Gupta et al., “Security and Privacy in Smart Farming: Challenges and Opportunities,” *IEEE Access* PP (19 Φεβρουαρίου 2020): 1–1, https://doi.org/10.1109/ACCESS.2020.2975142.

Εικόνα 9: Λίστα Κυβερνοεπιθέσεων



Πηγή:https://www.researchgate.net/profile/Maanak-Gupta/publication/339372082/figure/fig2/AS:860499470188547@1582170469390/A-Roadmap-of-Cybersecurity-Research-and-Challenges-in-Smart-Farming.ppm

Η παραπάνω εικόνα είναι μέρος μιας εργασίας για την Κυβερνοασφάλεια, την Ιδιωτικότητα και τις προκλήσεις στην Ευφυή Γεωργία των Maanak Gupta et al. Παρατίθεται το απόσπασμα που αναφέρεται στις κυβερνοεπιθέσεις και μόνο. Έχοντας εντρυφήσει στη σχετική βιβλιογραφία και στην αντίστοιχη βιομηχανική έρευνα[15], προκύπτει το συμπέρασμα ότι οι κυβερνοεπιθέσεις στον αγροτικό τομέα πρέπει να αντιμετωπίζονται και να εξετάζονται από την σκοπιά είτε των επιθέσεων σε βασικές υποδομές (utilities sector), είτε των επιθέσεων στο βιομηχανικό τομέα[16]. Συνεπώς, σε τέτοιου είδους κυβερνοεπιθέσεις δεν πρόκειται εύκολα να εντοπιστούν τεχνικές «ψαρέματος» (phishing) ή «κοινωνικής μηχανικής» (social engineering). Ο λόγος είναι ότι ο αγρότης δύσκολα θα έχει τεχνικές λεπτομέρειες του πληροφοριακού συστήματος Γεωργίας Ακριβείας που χρησιμοποιεί. Πιο πιθανό είναι ότι θα το έχει εγκαταστήσει κάποια εξειδικευμένη εταιρεία η οποία θα του έχει δώσει κάποια πρόσβαση σε μια Cloud εφαρμογή προκειμένου να λαμβάνει μετρήσεις, δεδομένα κτλ. Σε τέτοιες περιπτώσεις, οι επιθέσεις έχουν ως στόχο την ίδια την τεχνολογία και όχι κάποιον υπάλληλο ή χρήστη με κάποιες γνώσεις λειτουργίας του συστήματος. Παρακάτω με βάση τις σχετικές ερευνητικές εργασίες[17] [18] [19], παρουσιάζονται και αναλύονται οι ενδεχόμενες επιθέσεις.

[15] Πηγή: Zhanna Malekos Smith, Eugenia Lostri, and James A Lewis, “The Hidden Costs of Cybercrime,” n.d., 38.
[16] Πηγή: “Industrial Cyber Security Guide | ABB,” Industrial Software, Ανακτήθηκε στις 18 Ιουλίου 2022, https://new.abb.com/industrial-software/industrial-cyber-security-guide.
[17] Πηγή: Gupta et al., “Security and Privacy in Smart Farming.”

- **Επίθεση στα δεδομένα (Data Attacks)**
    - **Διαρροή δεδομένων από μέσα (Insider Data Leakage)**. Αυτού του είδους η επίθεση έχει ως αποτέλεσμα τη διαρροή ευαίσθητων δεδομένων προς τρίτους οι οποίοι δεν έχουν την εξουσιοδότηση να έχουν πρόσβαση σε αυτά τα δεδομένα. Συνήθως, αυτές οι επιθέσεις προϋποθέτουν τη συνέργεια ή σύμπραξη κάποιου προσώπου (συνηθέστερα ενός υπαλλήλου) από το μέσα κόσμο της επιχείρησης ή του οργανισμού. Δεν εκτελείται κάποιο είδος επίθεσης στην υπολογιστική υποδομή της επιχείρησης και ως εκ τούτου είναι αρκετά δύσκολο να γίνει αντιληπτό για να παρεμποδιστεί. Η επίπτωση σε αυτήν την περίπτωση έχει να κάνει με τη διαρροή ευαίσθητων δεδομένων, οικονομικής φύσης πολλές φορές, τα οποία μπορούν να προσφέρουν ανταγωνιστικό πλεονέκτημα στις άλλες επιχειρήσεις που δραστηριοποιούνται στον ίδιο τομέα. Συν τοις άλλοις, μετά από ένα τέτοιας φύσης περιστατικό διαρρηγνύεται ο ιστός εμπιστοσύνης των ανθρώπων μέσα στην ίδια την επιχείρηση.

    - **Διαρροή δεδομένων στο Cloud (Cloud Data Leakage).** Επιχειρήσεις, εταιρείες, κρατικά ιδρύματα και κυβερνητικοί οργανισμοί πάνε τα τελευταία χρόνια τις υπηρεσίες και τις υπολογιστικές τους υποδομές στο Cloud (IaaS, Infrastructure as a Service). Το Cloud με τη σειρά του αποτελείται από Data Centers τα οποία βρίσκονται διανεμημένα σε όλο τον κόσμο. Το πρόβλημα που μπορεί να παρουσιαστεί σε μία τέτοια περίπτωση έχει να κάνει με την διαρροή δεδομένων από ένα μολυσμένο κομμάτι λογισμικού που τρέχει σε κάποιο Virtual Server σε Data Center που μπορεί να βρίσκεται σε άλλη χώρα. Το αποτέλεσμα μπορεί να είναι καταστροφικό διότι, όπως και στην πιο πάνω περίπτωση έχουμε διαρροή ευαίσθητων δεδομένων προς ανταγωνιστικές χώρες, οργανισμούς, ή και εταιρείες. Τα δεδομένα αυτά μπορούν να δώσουν ένα στρατηγικό πλεονέκτημα σε αυτούς που θα τα αποκτήσουν. Αυτού του είδους η επίθεση περιλαμβάνει συνήθως και επίθεση προς την ίδια την τεχνολογία, αφού ο επιτιθέμενος μπόρεσε να αποκτήσει πρόσβαση εκμεταλλευόμενος κάποια αδυναμία του συστήματος ή του λογισμικού του. Λόγω της διανεμημένης φύσης του Cloud τα δεδομένα μπορεί να βρίσκονται σε κίνδυνο οποιαδήποτε στιγμή. Για αυτό το λόγο πολλές χώρες έχουν αρχίσει να περνάνε νόμους για την εντοπιότητα των ευαίσθητων δεδομένων. Με άλλα λόγια θα πρέπει δεδομένα που έχουν χαρακτηριστεί ως ευαίσθητα να φυλάσσονται μόνο σε servers που βρίσκονται στο έδαφος της ενδιαφερόμενης χώρας[20].

[18] Πηγή: Abbas Yazdinejad et al., "A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures," *Applied Sciences* 11 (August 16, 2021): 7518, https://doi.org/10.3390/app11167518.

[19] Πηγή: S. Sontowski et al., "Cyber Attacks on Smart Farming Infrastructure," 2020, 135–43, https://doi.org/10.1109/CIC50333.2020.00025.

[20] Πηγή: Shanhe Yi, Zhengrui Qin, and Qun Li, "Security and Privacy Issues of Fog Computing: A Survey," 2015, 685–95, https://doi.org/10.1007/978-3-319-21837-3_67.

- **Εισαγωγή ψευδών δεδομένων (False Data Injection Attack).** Μια τέτοια επίθεση έχει ως στόχο την εισαγωγή ψευδών ή παραποιημένων δεδομένων με σκοπό την παραγωγή αντίστοιχα παραποιημένων αποτελεσμάτων με σκοπό τη διακοπή ή και την ολοκληρωτική καταστροφή της παραγωγικής διαδικασίας μιας εταιρείας. Στο περιβάλλον της Γεωργίας Ακριβείας μια τέτοια επίθεση θα συνιστούσε στην εισαγωγή παραποιημένων τιμών υγρασίας εδάφους μιας καλλιέργειας με αποτέλεσμα είτε την υπερβολική άρδευση, είτε τη μείωση της εισροής νερού. Σε κάθε περίπτωση η επίπτωση θα ήταν η καταστροφή της καλλιέργειας.

- **Παραπληροφόρηση (Misinformation Attack).** Πρόκειται για επίθεση σε αυτό που ονομάζουμε ακεραιότητα των δεδομένων (data integrity). Υπάρχουν αρκετοί τρόποι και μέθοδοι για να διαπραχθεί μια τέτοια επίθεση. Στην περίπτωση της γεωργίας ο επιτιθέμενος θα μπορούσε να δημοσιεύσει μια αναφορά η οποία θα προσομοίαζε μια πραγματική αναφορά από μια έξυπνη φάρμα και η οποία θα έκανε λόγο για τη μη τήρηση προτύπων ασφάλειας και υγείας που οδηγούν σε κίνδυνο για τη δημόσια υγεία. Καθίσταται σαφές ότι σε αυτήν την περίπτωση πλήττεται ανεπανόρθωτα η υπόληψη και το όνομα της επιχείρησης.

- **Επίθεση στον υλικοτεχνικό και δικτυακό εξοπλισμό (Networking and Equipment Attacks).**
  - **Παρενόχληση σε επίπεδο ραδιοσημάτων (Radio Frequency Jamming Attack).** Πρόκειται για επίθεση η οποία στοχεύει κατευθείαν στην τεχνολογία. Πιο συγκεκριμένα, οι πιο πολλές από τις συσκευές - μηχανήματα στο ανοιχτό περιβάλλον του αγρού κάνουν χρήση ραδιοσυχνοτήτων για τηλεπικοινωνία, εύρεση θέσης, αποφυγή εμποδίων κτλ. Οι επιτιθέμενοι σε αυτού του είδους την επίθεση κάνουν χρήση κάποιων φορητών συσκευών οι οποίες ονομάζονται παρεμβολείς σήματος (jammers). Οι συσκευές αυτές είχαν πρώτη φορά χρησιμοποιηθεί για στρατιωτικούς σκοπούς για να παρεμβάλλουν στις τηλεπικοινωνίες του εχθρού και να τις διακόπτουν. Την ίδια ακριβώς δουλειά κάνουν και σε αυτήν την περίπτωση. Έτσι για παράδειγμα, ο επιτιθέμενος δύναται να χρησιμοποιήσει μια τέτοια συσκευή προκειμένου να διακόψει το σήμα GPS (Global Positioning System) ενός αυτόνομου ρομποτικού ψεκαστικού μηχανήματος ή τη σύνδεση των διαφόρων αισθητήρων με το δίκτυο. Δεν θεωρείται μεγάλης κλίμακας επίθεσης πια, διότι οι περισσότεροι αισθητήρες, όπως και τα περισσότερα αυτόνομα αγροτικά ρομποτικά οχήματα έχουν τη δυνατότητα να αλλάζουν αυτόματα συχνότητα (frequency hopping) όταν διαγνώσουν τέτοια κατάσταση. Επιπλέον, εφαρμόζοντας τεχνικές που χρησιμοποιούνται σε συστήματα συναγερμών, οι διάφορες συσκευές IoT Πυλών (IoT Gateways), χρησιμοποιούν μια δεύτερη ενσύρματη όδευση προκειμένου να

στείλουν σε μια εφαρμογή ειδοποίηση για τη σχετική κατάσταση που παρουσιάστηκε[21].

Εικόνα 10: Συσκευή IoT Πυλών

Πηγή: https://i.mt.lv/cdn/rb_images/2035_hi_res.png

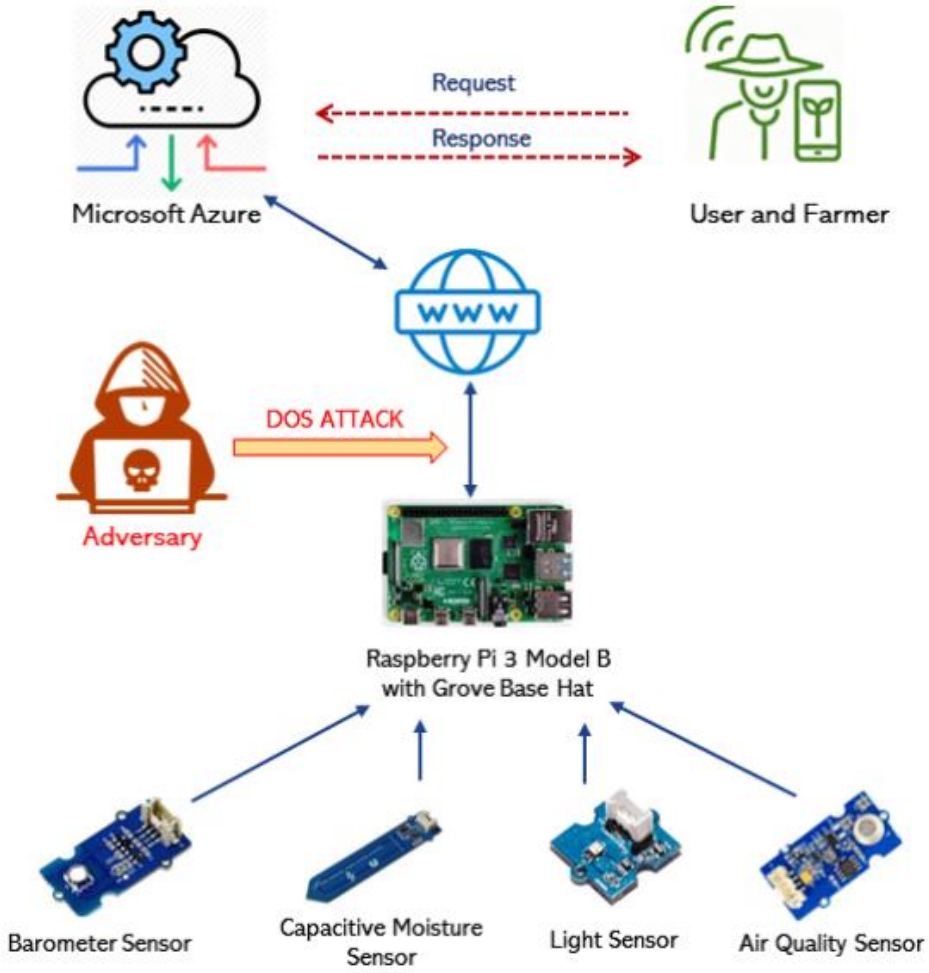
- **Εισαγωγή κακόβουλου λογισμικού (Malware Injection Attack).** Πρόκειται για μια από τις χειρότερές μορφές κυβερνοεπίθεσης. Η ζημιά που προκαλεί είναι πολύ μεγάλη και μπορεί να οδηγήσει ακόμη και σε διακοπή της καθημερινής λειτουργίας μιας μικρής ή και μεγάλης φάρμας. Το κακόβουλο λογισμικό είναι ένας ιδιαίτερος τύπος επικίνδυνου λογισμικού το οποίο με τον καιρό έχει εξελιχθεί σημαντικά ώστε νεότερες παραλλαγές του να μπορούν να ξεφεύγουν από τα τυπικά IDS/IPS (Intrusion Detection / Prevention Systems) συστήματα. Αυτού του είδους το λογισμικό μπορεί να μολύνει τους virtual servers όπου βρίσκονται εγκατεστημένες οι cloud εφαρμογές της Γεωργίας Ακριβείας. Μέσω αυτού ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση τόσο σε πολύτιμα δεδομένα μιας φάρμας, όπως οικονομικά στοιχεία, στοιχεία προσωπικού κτλ, όσο και πρόσβαση στο πληροφοριακό σύστημα και την υποδομή IoT που χρησιμοποιεί. Η πρόσβαση σε ευαίσθητα δεδομένα εγκυμονεί κινδύνους διαρροής τους σε ανταγωνιστικές φάρμες. Πιο συγκεκριμένα, η πρόσβαση στις εφαρμογές Γεωργίας Ακριβείας που χρησιμοποιεί μια έξυπνη φάρμα ή στην υποδομή IoT εγκυμονεί κινδύνους καταστροφής του εξοπλισμού. Ακόμη χειρότερα το κακόβουλο λογισμικό μπορεί να αποκτήσει πρόσβαση στην IoT υποδομή και να μετατρέψει τις συσκευές ή τα μηχανήματα σε botnets προκειμένου να εξαπολύσει επίθεση σε άλλους στόχους.

- **Άρνηση Παροχής Υπηρεσίας (Denial of Service Attack).** Οι συσκευές IoT καθώς και τα αυτόνομα ρομποτικά μηχανήματα που χρησιμοποιούνται σε μία έξυπνη φάρμα, παρουσιάζουν τις ίδιες ευπάθειες που παρουσιάζουν και οι άλλες συσκευές IoT που

[21] Πηγή: "MikroTik," ανακτήθηκε στις 19 Ιουλίου 2022, https://mikrotik.com/.

χρησιμοποιούνται στη βιομηχανία ή και στα λεγόμενα έξυπνα σπίτια. Τα χαρακτηριστικά ασφαλείας τους είναι από ανύπαρκτα έως και ιδιαίτερα φτωχά. Αυτό δεν είναι τυχαίο, καθώς οι περισσότεροι κατασκευαστές χρησιμοποιούν κοινά κομμάτια κώδικα μεταξύ τους, μια πρακτική η οποία τους επιτρέπει δραστική μείωση του κόστους. Συνεπώς, μια ευπάθεια (vulnerability) σε ένα από αυτά τα κομμάτια κώδικα, εγκυμονεί κινδύνους για τις περισσότερες IoT συσκευές που βρίσκονται στην αγορά. Επίσης, η ενσωμάτωση χαρακτηριστικών ασφαλείας στον βασικό τους κώδικα είναι κάτι το οποίο οδηγεί σε μεγαλύτερες απαιτήσεις σε επεξεργαστική ισχύ από την IoT συσκευή με αποτέλεσμα αυξημένη κατανάλωση ενέργειας και συνεπακόλουθα μειωμένη αυτονομία. Αυτές τις εγγενείς αδυναμίες εκμεταλλεύονται οι επιτιθέμενοι οι οποίοι μπορούν να πάρουν τον έλεγχο των IoT συσκευών προκειμένου να εξαπολύσουν επιθέσεις τύπου DoS (Denial of Service) σε άλλους στόχους. Επειδή οι συσκευές IoT σε μια έξυπνη φάρμα είναι εκπροοιμίου πολλές και αναμένεται να πληθύνουν στο πολύ άμεσο μέλλον προκειμένου να καλύψουν τις ανάγκες μιας καλλιέργειας, αποτελούν το καλύτερο εργαλείο για τους επιτιθέμενους προκειμένου να εξαπολύσουν μεγάλης κλίμακας επιθέσεις σε άλλους στόχους. Εξυπακούεται ότι σε τέτοια περίπτωση η λειτουργία μιας έξυπνης φάρμας καθίσταται προβληματική, με άμεσο κίνδυνο την πιθανή καταστροφή της καλλιέργειας.

Εικόνα 11: Επίθεση Άρνησης Παροχής Υπηρεσίας σε Έξυπνη Φάρμα

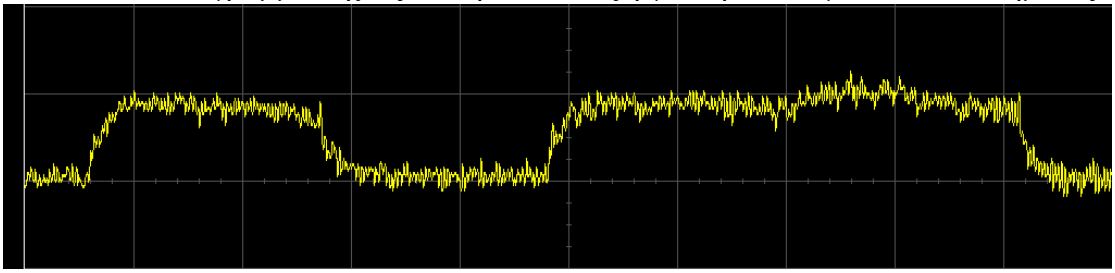


Πηγή: https://ebiquity.umbc.edu/_file_directory_/papers/1031.pdf

- **Botnets.** Πρόκειται για ένα τύπο επίθεσης που ξεκίνησε από το βιομηχανικό χώρο εφαρμογής των IoT, εξαπλώθηκε στα έξυπνα σπίτια, ενώ φυσικά αποτελεί ιδανικό πεδίο εφαρμογής και στη Γεωργία Ακριβείας με τους δεκάδες αισθητήρες και αυτόνομους ρομποτικούς μηχανισμούς στον αγρό. Αυτός ο τύπος επίθεσης χρησιμοποιείται για να υλοποιηθεί η επίθεση τύπου DoS (Denial of Service). Αυτό καθίσταται εφικτό με το μηχανισμό που περιγράφηκε πιο πάνω. Δηλαδή, ο επιτιθέμενος εκμεταλλευόμενος μια εγγενή τους αδυναμία στον τομέα της ασφάλειας, αποκτάει τον έλεγχο και τις συντονίζει όλες μαζί για μαζική επίθεση σε άλλους στόχους. Σύμφωνα με την εργασία[22] οι επιθέσεις τύπου botnet θα τείνουν να γίνονται όλο και πιο συνηθισμένες σε αγροτικά περιβάλλοντα.

- **Side Channel Επιθέσεις.** Αποτελεί μια από τις πιο δύσκολες, όσον αφορά την υλοποίησή της, τεχνικά επιθέσεις. Ο σχεδιασμός και η εφαρμογή της προϋποθέτει πολύ καλή έως και άριστη γνώση του συστήματος και της υποδομής. Ο επιτιθέμενος δεν εκμεταλλεύεται κάποια αδυναμία του συστήματος, αλλά περισσότερο κάποιο πρωτόκολλο ή κάποια λειτουργία του συστήματος. Για παράδειγμα, από το θόρυβο του χτυπήματος των πλήκτρων του πληκτρολογίου είναι δυνατόν να «αποκρυπτογραφηθούν» ποιά πλήκτρα πατιούνται και έτσι να υποκλαπούν κωδικοί και συνθηματικά τελικών χρηστών. Στην παρακάτω εικόνα[23] απεικονίζεται το διάγραμμα ισχύος του κεντρικού επεξεργαστή ενός υπολογιστικού συστήματος, όταν αυτός ξεκινάει τη διαδικασία αποκωδικοποίησης ενός κωδικού κρυπτογραφημένου με αλγόριθμό RSA.

Εικόνα 12: Διάγραμμα Ισχύος Κεντρικού Επεξεργαστή Υπολογιστικού Συστήματος



Πηγή: https://upload.wikimedia.org/wikipedia/commons/6/6c/Power_attack.png

Η αριστερή ανύψωση της κυματομορφής δείχνει τις διακυμάνσεις στην ενέργεια του κεντρικού επεξεργαστή καθώς αυτός ξεκινάει τη διαδικασία αποκωδικοποίησης. Με βάση αυτό ένας επιτιθέμενος μπορεί να διαβάσει την ακολουθία των bits. Στην παραπάνω εικόνα έχουμε τα bits 0, 1. Γενικά, τέτοιου

[22] Πηγή: Sontowski et al., "Cyber Attacks on Smart Farming Infrastructure."
[23] Πηγή: "Side-Channel Attack," στην *Wikipedia*, 7 Ιουνίου 2022, https://en.wikipedia.org/w/index.php?title=Side-channel_attack&oldid=1092051943.

είδους επιθέσεις είναι ιδιαίτερα δύσκολες είτε στο αγροτικό, είτε σε οποιαδήποτε άλλο πεδίο.

Οι επιθέσεις που περιγράψαμε παραπάνω χρησιμοποιούνται με κάποιες διαφοροποιήσεις σε μεθοδολογία και τεχνικές, και σε στάδια που δεν άπτονται της Γεωργίας Ακριβείας. Εντούτοις μπορούν να προξενήσουν αρκετή ζημιά πέραν μίας αγροτικής επιχείρησης ακόμα και σε μια ολόκληρη χώρα. Πρόκειται για επιθέσεις στις υπολογιστικές υποδομές της εφοδιαστικής αλυσίδας. Το κομμάτι αυτό βρίσκεται εκτός της θεματικής ενότητας που εξετάζεται οπότε δε θα υπάρξει περαιτέρω επέκταση. Ωστόσο, αναδεικνύεται πως επιθέσεις αυτού του τύπου μπορεί να έχουν μεγάλο αντίκτυπο σε μια αγροτική επιχείρηση. Έστω ότι η επίθεση περιλαμβάνει αλλοίωση των δεδομένων των IoT αισθητήρων που παρακολουθούν τη θερμοκρασία και υγρασία του φορτίου από τον αγρό προς τα σημεία πώλησης. Τότε, υπάρχει περίπτωση το φορτίο να έχει αλλοιωθεί κατά τρόπο επιζήμιο για την δημόσια υγεία. Όταν αυτό γίνει αντιληπτό και μέχρι να εξακριβωθεί η πραγματική φύση του συμβάντος η αγροτική επιχείρηση θα έχει υποστεί ένα σημαντικό πλήγμα στην ακεραιότητά της[24]. Σε επίπεδο χώρας μια κυβερνοεπίθεση στην υπολογιστική υποδομή της εφοδιαστικής αλυσίδας δύναται να σημάνει την κατάρρευση της αγοράς τροφίμων με αποτέλεσμα μια μικρής ή και μεγάλης κλίμακας επισιτιστική κρίση[25].

1.7 Επιθέσεις APT (Advanced Persistent Threat)

Σε αυτό το σημείο, κρίνεται σκόπιμη η μελέτη και ενδελεχής ανάλυση των επιθέσεων τύπου APT (Advanced Persistent Threat). Ο λόγος έχει να κάνει με την ένταση και τη διάρκεια μιας επίθεσης τύπου APT[26] και τον αντίκτυπο που αυτή η επίθεση έχει κυρίως σε αγροκτήματα που εφαρμόζουν μεθόδους, τακτικές και τεχνολογίες Γεωργίας Ακριβείας.

Ο όρος APT χρησιμοποιείται για να περιγράψει μια επιθετική εκστρατεία από μια ομάδα επιτιθέμενων προκειμένου να καταφέρουν να αποκτήσουν και να εγκαθιδρύσουν μια μακράς διάρκειας παραμονή σε μια δικτυακή υπολογιστική υποδομή, ώστε σταδιακά να υποκλέψουν ευαίσθητα δεδομένα[27]. Αυτού του είδους οι επιθέσεις χαρακτηρίζονται από τον προσεκτικό σχεδιασμό και την επιλογή των στόχων, οι οποίοι στην πλειοψηφία των περιπτώσεων αποτελούν μεγάλες εταιρείες ή οργανισμοί, κυβερνητικοί ή ιδιωτικοί. Οι επιπτώσεις μιας τέτοιου τύπου εισβολής είναι σοβαρές και αρκετές φορές μη αναστρέψιμες. Συγκεκριμένα:

- Κλοπή δεδομένων πνευματικής ιδιοκτησίας, όπως πατέντες, εμπορικά μυστικά, εκθέσεις και αναφορές κ.α.
- Κλοπή ευαίσθητων δεδομένων
- Καταστροφή εξοπλισμού και υποδομών

Στην προκειμένη περίπτωση, δηλαδή, στις επιχειρήσεις που δραστηριοποιούνται στον αγροτικό τομέα και εφαρμόζουν τεχνικές ακριβούς γεωργίας έχουμε:

[24] Πηγή: Yazdinejad et al., "A Review on Security of Smart Farming and Precision Agriculture."
[25] Πηγή: Angyalos, Botos, and Robert, "The Importance of Cybersecurity in Modern Agriculture."
[26] Πηγή: "What Is APT (Advanced Persistent Threat) | APT Security | Imperva," *Learning Center* (blog), Ανακτήθηκε στις 19 Ιουλίου 2022, https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.
[27] "What Is APT (Advanced Persistent Threat) | APT Security | Imperva."

- Πιθανή ολοκληρωτική καταστροφή αγροτικών καλλιεργειών
- Καταστροφή πανάκριβου εξοπλισμού, όπως τα αυτόνομα εναέρια ρομποτικά συστήματαπου χρησιμοποιούνται για επιτήρηση, φασματοσκοπική φωτογράφηση και τηλεμετρία

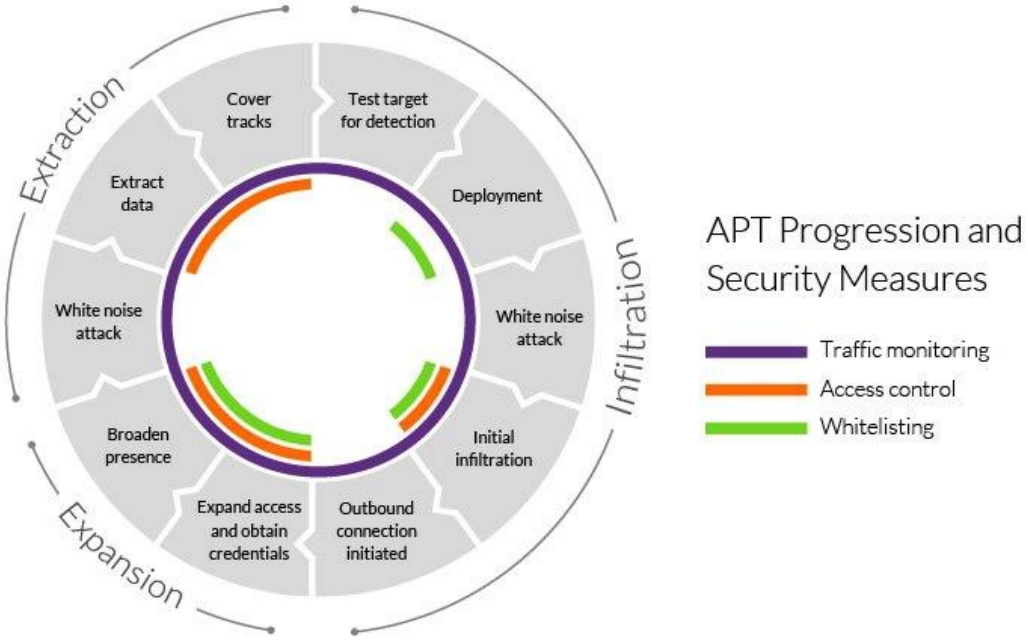
Οι επιθέσεις τύπου APT όπως αναδεικνύεται, είναι πολύ καλά οργανωμένες. Οι στόχοι επιλέγονται πολύ προσεκτικά και η επίθεση έχει μεγάλη διάρκεια. Οι επιτιθέμενοι έχουν υψηλό γνωστικό υπόβαθρο της τεχνολογίας που χρησιμοποιούν και επίσης πολύ καλή γνώση του επιλεγμένου στόχου. Η παρουσία τους, όταν γίνει αντιληπτή, θα είναι γιατί οι ίδιοι οι επιτιθέμενοι έχουν επιλέξει να την αποκαλύψουν[28]. Η επίθεση τύπου APT πραγματοποιείται σταδιακά σε διακριτά βήματα:

- Διείσδυση
  Οι επιτιθέμενοι συνηθέστερα προσπαθούν να εκμεταλλευτούν αδυναμίες των επιχειρήσεων στους εξής πόρους: ιστοτόπους, δικτυακή υποδομή και στο ανθρώπινο δυναμικό. Σε επιχειρήσεις που δραστηριοποιούνται στο τομέα της Γεωργίας Ακριβείας η καλύτερη επιφάνεια προσβολής (attack surface) είναι χωρίς αμφιβολία η IoT υποδομή, καθώς το οικοσύστημα των συσκευών IoT χαρακτηρίζεται από φτωχή, αν όχι από ανεπαρκή υποδομή ασφάλειας.
- Εγκαθίδρυση
  Από τη στιγμή που οι επιτιθέμενοι έχουν διεισδύσει εντός του οργανισμού, τότε ασχολούνται με το να καταγράφουν και να γνωρίζουν όλους τους διαθέσιμους πόρους της υπολογιστικής υποδομής μιας επιχείρησης. Σε αυτό το στάδιο θα ξεκινήσουν να αντιγράφουν ευαίσθητα δεδομένα, όπως λόγου χάρη στοιχεία για το προσωπικό ή εμπορικές συμφωνίες, αλλά σε κάποια ασφαλή δικτυακή τοποθεσία εντός του οργανισμού. Πέραν αυτού, οι προσπάθειές τους θα επικεντρώνονται στη δημιουργία κακόβουλου λογισμικού που θα τους βοηθήσει να φτιάξουν «κερκόπορτες» (backdoors) σε πολλαπλά σημεία εισόδου – εξόδου της δικτυακής υποδομής. Λογικά στις επιχειρήσεις που εμπλέκονται με την ευφυή γεωργία, οι κερκόπορτες θα βρίσκονται είτε στην Cloud υποδομή, είτε θα γίνεται χρήση σημείων εισόδου – εξόδου του LP – WAN δικτύου των IoT συσκευών. Είναι σημαντικό να τονιστεί ότι τα παραπάνω εκτελούνται χωρίς να γίνεται κάτι αντιληπτό είτε από κάποιο σύστημα ασφαλείας είτε από κάποιον από το προσωπικό.
- Εξαγωγή
  Σε αυτό το στάδιο οι επιτιθέμενοι έχουν μαζέψει τα δεδομένα που τους είναι πολύτιμα, έχουν εγκαθιδρύσει τις κερκόπορτες τους στην δικτυακή υποδομή και πλέον μπορούν να κάνουν εξαγωγή των υποκλεμμένων δεδομένων. Προκειμένου να μη γίνει ή όλη διαδικασία αντιληπτή μπορεί να καταφύγουν σε τεχνικές αντιπερισπασμού[29]. Πρόκειται για τεχνικές «λευκού θορύβου» (white noise tactics), όπως λόγου χάρη επιθέσεις τύπου DoS (Denial of Service) προς την ίδια την επιχείρηση, οι οποίες κινητοποιούν και συνεπακόλουθα κρατούν απασχολημένο το προσωπικό, προκειμένου να μη γίνει αντιληπτή η εξαγωγή δεδομένων[30].Ο μεγάλος κίνδυνός από τις επιθέσεις

[28] Πηγή: “What Is an Advanced Persistent Threat (APT)?,” www.kaspersky.com, February 9, 2022, https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.
[29] Πηγή: “What Is APT (Advanced Persistent Threat) | APT Security | Imperva.”
[30] Πηγή: “What Is an Advanced Persistent Threat (APT)?”

τύπου APT δεν έγκειται μόνο στην υποκλοπή των δεδομένων ή όποιας άλλης ζημιάς στις υποδομές, αλλά πολύ περισσότερο, ότι ακόμη κι αν γίνει αντιληπτή η εισβολή και η άμεση απειλή εξουδετερωθεί, υπάρχει πάντοτε ο κίνδυνος να έχουν μείνει στην υπολογιστική και δικτυακή υποδομή κερκόπορτες οι οποίες μελλοντικά θα χρησιμοποιηθούν για επιπλέον εισβολές. Παρακάτω απεικονίζεται η εξέλιξη μιας APT επίθεσης μαζί με πιθανά μέτρα αντιμετώπισης.

Εικόνα 13: Εξέλιξη APTεπίθεσης και Μέτρα Ασφάλειας



Πηγή: https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/apt-advanced-persistent-threat-security.jpg.webp

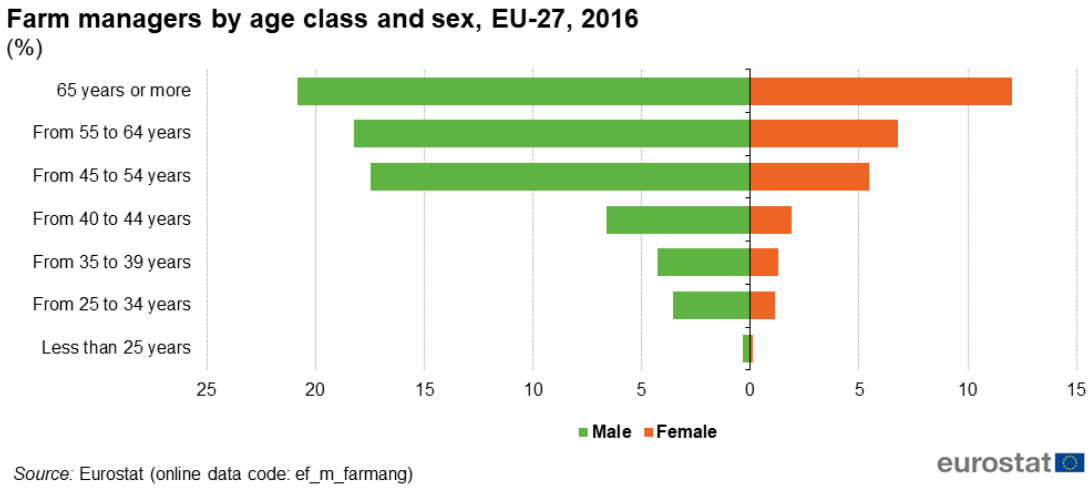
1.8 Αντίμετρα

Στη βιβλιογραφία για την κυβερνοασφάλεια υπάρχουν αμέτρητες εργασίες σχετικά με τις πρακτικές και τις τεχνολογίες στις οποίες μπορεί να επενδύσει κάποιος οργανισμός ή επιχείρηση για να αισθάνεται και να είναι ασφαλής στην ψηφιακή εποχή. Εκτός αυτού υπάρχουν και εταιρείες εξειδικευμένες στην παροχή τεχνολογίας και τεχνογνωσίας προκειμένου η υπολογιστική και δικτυακή υποδομή μιας εταιρείας, μιας επιχείρησης ή ενός οργανισμού να θωρακιστεί αποτελεσματικά απέναντι σε τέτοιου είδους απειλές.

Ωστόσο, η περίπτωση των επιχειρήσεων ή εταιρειών που δραστηριοποιούνται στον αγροτικό κλάδο κάνοντας χρήση τεχνικών και τεχνολογιών ευφυούς γεωργίας, παρουσιάζει ιδιάζουσα αντιμετώπιση. Καταρχήν, είναι δύσκολο να επικοινωνηθεί η σημασία της κυβερνοασφάλειας όταν ο περισσότερος κόσμος που εμπλέκεται με τη διαχείριση αυτού του είδους των επιχειρήσεων έχει ηλικία μεγαλύτερη των 55 ετών[31].

[31] Πηγή: “Farmers and the Agricultural Labour Force - Statistics,” Ανακτήθηκε στις 19 Ιουλίου 2022, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Farmers_and_the_agricultural_labour_force_-_statistics.

Εικόνα 14: Ηλικία και φύλο εμπλεκομένων στον αγροτικό τομέα στην Ευρώπη



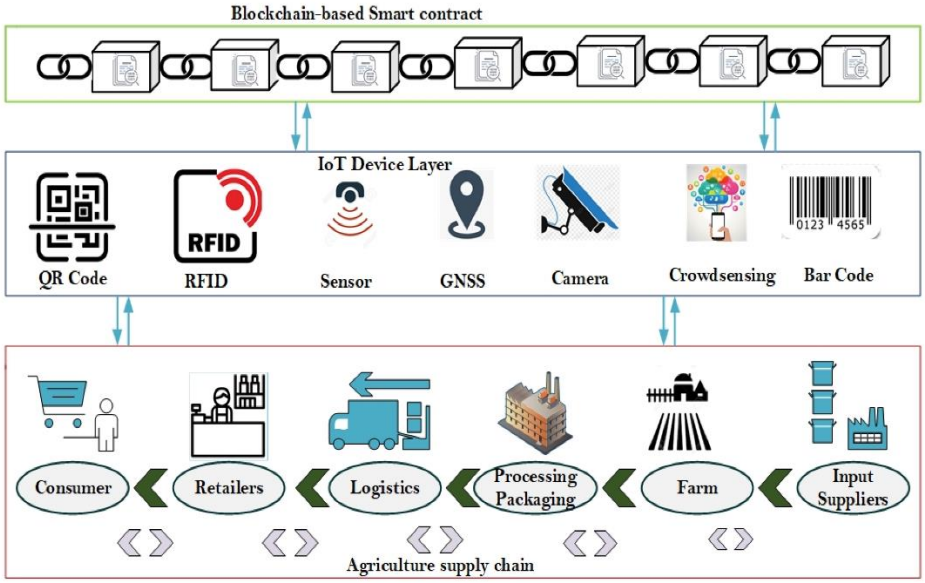
Πηγή: https://ec.europa.eu/eurostat/statistics-explained/images/5/52/Farm_managers_by_age_class_and_sex%2C_EU-27%2C_2016_%28%25%29_FP20.png

Οι περισσότερες από τις έρευνες που εξετάστηκαν, εξαντλούνται σε συνήθη τεχνολογικά εργαλεία, όπως συστήματα IDS / IPS (Intrusion Detection / Intrusion Prevention Systems) ή πρακτικές ασφαλείας (best practices) όπως συχνές αλλαγές των κωδικών ασφαλείας, αποφυγή ανοίγματος email που είναι ύποπτα κτλ. Ωστόσο, καμία από τις εργασίες δεν λαμβάνει σοβαρά υπόψη το γεγονός ότι οι συσκευές IoT που έχουν κατακλύσει την αγορά και είναι αυτές που οδηγούν τις εξελίξεις σχετικά με την Ευφυή Γεωργία, παραμένουν ο πιο αδύναμος κρίκος στην αλυσίδα της κυβερνοασφάλειας. Συνεπώς ως λήψη αντιμέτρων ασφαλείας κρίνονται απαραίτητα τα εξής:

- Θωράκιση των IoT συσκευών. Επειδή όπως προειπώθηκε τα χαρακτηριστικά ασφαλείας τους είναι από φτωχά έως και ανεπαρκή, οι κατασκευαστές τους πρέπει να μεριμνήσουν έτσι ώστε από το σχεδιασμό τους να έχουν χαρακτηριστικά ασφαλείας τα οποία:
    - Να είναι εγγενή, δηλαδή θα περιλαμβάνονται μέσα στον κώδικα της συσκευής.
    - Να υπάρχει δυνατότητα συχνών ενημερώσεων ασφαλείας από τον ίδιο τον κατασκευαστή.
- Χρήση IoT gateway, δηλαδή να μη βγαίνει η κάθε IoT συσκευή στο διαδίκτυο, αλλά να υπάρχει μια συσκευή η οποία να επικοινωνεί μέσω τεχνολογίας LP-WAN με τις υπόλοιπες συσκευές και μέσω αυτής να επικοινωνούν με το Cloud. Τα IoT gateways παρέχουν αρκετά χαρακτηριστικά ασφαλείας, με τα πιο ακριβά από αυτά να έχουν IDS / IPS λειτουργίες καθώς και anti – jamming τεχνολογίες.
- Blockchain. Εκτιμάται πως η τεχνολογία Blockchain αποτελεί τη πλέον ιδανική λύση στο θέμα της Κυβερνοασφάλειας για τη Γεωργία Ακριβείας. Ως τεχνολογία είναι πλέον ώριμη αφού έχει αρχίσει να εφαρμόζεται από αρκετές χρηματοοικονομικές εταιρείες προκειμένου να διασφαλίσει την ακεραιότητατων δεδομένων τωνσυναλλαγών. Η τεχνολογία Blockchain

μπορεί να εφαρμοστείαπό το επίπεδο ενός αισθητήρα IoT μέχρι το προϊόν να φτάσει στον τελικό καταναλωτή[32].

Εικόνα 15: Τεχνολογία Blockchain στην Γεωργία Ακριβείας



Πηγή: https://www.mdpi.com/agriculture/agriculture-12-00040/article_deploy/html/images/agriculture-12-00040-g003.png

Στην Ευφυή Γεωργία η τεχνολογία Blockchain έχει ευρύ πεδίο εφαρμογής[33]. Πετυχαίνει να εισάγει δυνατότητες εξελιγμένης ιχνηλασιμότητας, από το φυτό μέχρι και το πιάτο του τελικού καταναλωτή, χωρίς κεντρικό έλεγχο και κυρίως χωρίς να απαιτεί την apriori εμπιστοσύνη των συμβαλλόμενων μερών. Ωστόσο, απαιτείται αρκετή έρευνα και συμφωνία ως προς την υιοθέτηση ενός κοινού πλαισίου εφαρμογής της τεχνολογίας Blockchain.

1.9 Συμπεράσματα 1ου Κεφαλαίου – Μελλοντικές Τάσεις

Η χρήση τεχνολογιών IoT αποτελεί μονόδρομο για την επιτυχημένη εφαρμογή της Γεωργίας Ακριβείας. Ωστόσο, η τεχνολογία IoT ακόμη παρουσιάζει εγγενείς αδυναμίες, αναφορικά με την ασφάλεια απέναντι σε κυβερνοεπιθέσεις.

Στη συγκεκριμένη εργασία, αναλύθηκαν οι πιθανές κυβερνοεπιθέσεις σε δεδομένα και δικτυακό εξοπλισμό, ενώ παρουσιάστηκαν οι επιπτώσεις, αναφορικά με την Γεωργία Ακριβείας. Αναλύθηκε μία από τις πιο επικίνδυνες επιθέσεις, η APT και παρατέθηκαν οικίνδυνοι που εγκυμονούνται στον αγροτικό κλάδο, καθώς και οι επιπτώσεις, πάντοτε αναφορικά με την ευφυή γεωργία. Τέλος, προτάθηκαν πιθανά αντίμετρα – λύσεις που μπορούν να υλοποιηθούν και να εφαρμοστούν με επιτυχία.

Αυτό που πρέπει να τονιστεί και να κατανοηθεί, είναι ότι οι συνέπειες μιας κυβερνοεπίθεσης σε μια επιχείρηση που εμπλέκεται στην αγροτικό κλάδο έχουν διαφορετική υφή και βαρύτητα σε σχέση με επιχειρήσεις σε άλλους τομείς. Πιο αναλυτικά, μια κυβερνοεπίθεση σε μια άλλη εταιρεία θα έχει ως τελικές συνέπειες:

[32] Πηγή: Showkat Ahmad Bhat et al., “Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability,” *Agriculture* 12, no. 1 Ανακτήθηκε 10 Ιουνίου 2022: 40, https://doi.org/10.3390/agriculture12010040.

[33] Πηγή: Praveen Pappula et al., “Smart Farming: Securing Farmers Using Block Chain Technology and IOT,” 2021, 225–38, https://doi.org/10.1007/978-3-030-65691-1_15.

1. Υποκλοπή ευαίσθητων δεδομένων.
2. Μερική ή και πλήρη διακοπή της λειτουργίας της επιχείρησης για κάποιο χρονικό διάστημα. Σε κάθε περίπτωση, αν υπάρχει σωστή πολιτική κράτησης αντιγράφων ασφαλείας (backup) η επιχείρηση μπορεί να επανέλθει σχεδόν πλήρως σε διάστημα λίγων ημερών.
3. Οικονομική ζημιά.

Αντίθετα, μία επιχείρηση που δραστηριοποιείται στον αγροτικό τομέα θα έχει ως τελικές συνέπειες μίας κυβερνοεπίθεσης:

1. Υποκλοπή ευαίσθητων δεδομένων.
2. Πιθανή καταστροφή εξοπλισμού, όπως τα αυτόνομα εναέρια οχήματα παρακολούθησης και φασματομετρικής καταγραφής.
3. Πιθανή διακοπή της επιχείρησής για μακρό χρονικό διάστημα, αν λόγω της κυβερνοεπίθεσης καταστραφεί η καλλιέργεια.
4. Διαρρηγνύεται η σχέση εμπιστοσύνης της επιχείρησης με τον τελικό καταναλωτή. Εφόσον, το παραγόμενο προϊόν είναι τροφή και η επίθεση έβλαψε την ποιότητα του, τότε η εμπιστοσύνη του καταναλωτή κλονίζεται με τρόπο πολλές φορές ανεπανόρθωτο.

Τέλος, όσον αφορά το μέλλον, φαίνεται πως η λύση της τεχνολογίας Blockchain θα αποτελέσει το κλειδί στην εξασφάλιση αντίμετρων απέναντι στις κυβερνοεπιθέσεις. Στο επόμενο κεφάλαιο θα αναλυθεί ενδελεχώς στον τομέα των Logistics.

Πανεπιστήμιο Πειραιώς
University of Piraeus

Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Κλιματική Κρίση και Τεχνολογίες Πληροφορικής και Επικοινωνιών

Κεφάλαιο 2

Τεχνολογία Blockchain στα Logistics

Πειραιάς
2023

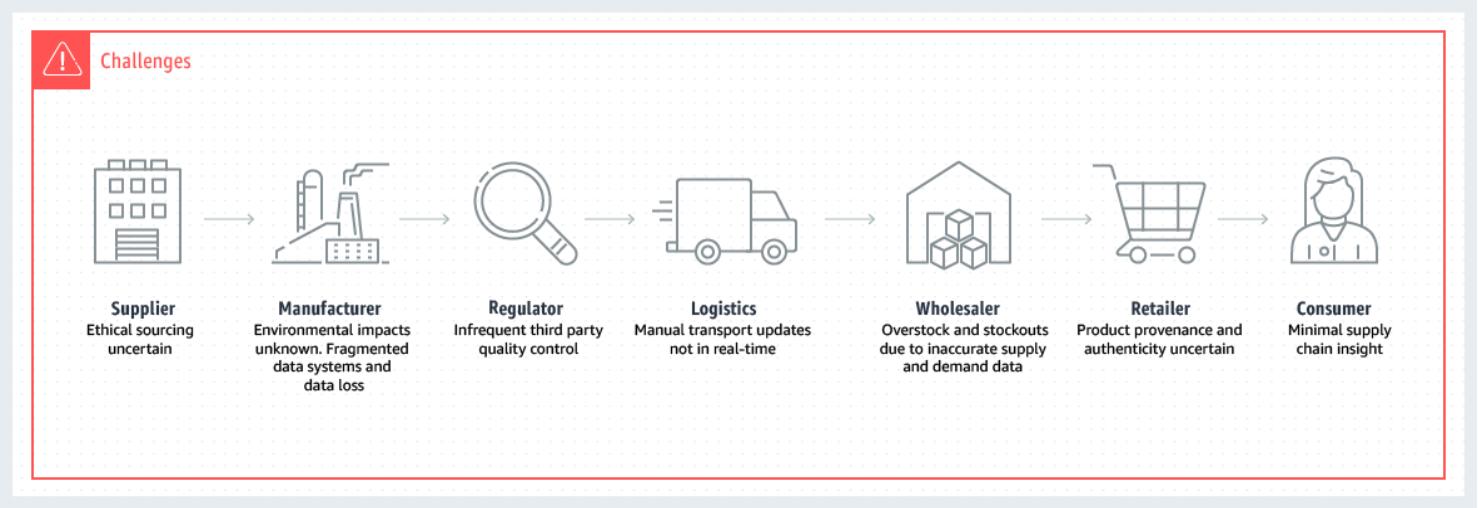
2.1 Εισαγωγή 2ου Κεφαλαίου

Η Blockchain είναι μια αναδυόμενη τεχνολογική ιδέα που επιτρέπει την αποκεντρωμένη και αμετάβλητη αποθήκευση επαληθευμένων δεδομένων. Τα τελευταία χρόνια, έχει προσελκύσει όλο και περισσότερο την προσοχή διαφορετικών βιομηχανιών.

Εφευρέθηκε από τον ή τους Satoshi Nakamoto, ένα ή περισσότερα μυστηριώδη άτομα που δεν έχουν αποκαλυφθεί μέχρι σήμερα. Η τεχνολογία έγινε γνωστή στο ευρύ κοινό τον Σεπτέμβριο του 2015 όταν εννέα χρηματοοικονομικές εταιρείες – GoldmanSachs, Barclays, J.P. Morgan και άλλοι – ένωσαν τις δυνάμεις τους για να δημιουργήσουν μια νέα υποδομή βασισμένη στη Blockchain για χρηματοοικονομικές υπηρεσίες.[34]

Σύμφωνα με την Beata Javorcik, επικεφαλής οικονομολόγο της Ευρωπαϊκής Τράπεζας Ανασυγκρότησης και Ανάπτυξης, η Ελλάδα έχει τη δυνατότητα να επωφεληθεί από τη συνεχιζόμενη διεθνή οικονομική αναδιάρθρωση προσελκύοντας νέες επενδύσεις και δημιουργώντας νέες ευκαιρίες απασχόλησης. Επιπρόσθετα, τονίζεται ότι η πρωταρχική προσέγγιση της EBRD προς την Ελλάδα περιλαμβάνει τη στενή συνεργασία με τις αρχές και τους ιδιώτες επενδυτές σε διάφορα έργα που στοχεύουν στην ενίσχυση των Logistics και των ενεργειακών συνδέσεων της Ελλάδας με τις γειτονικές της χώρες στη νοτιοανατολική Ευρώπη.[35]

Εικόνα 16: Προκλήσεις στον τομέα των Logistics



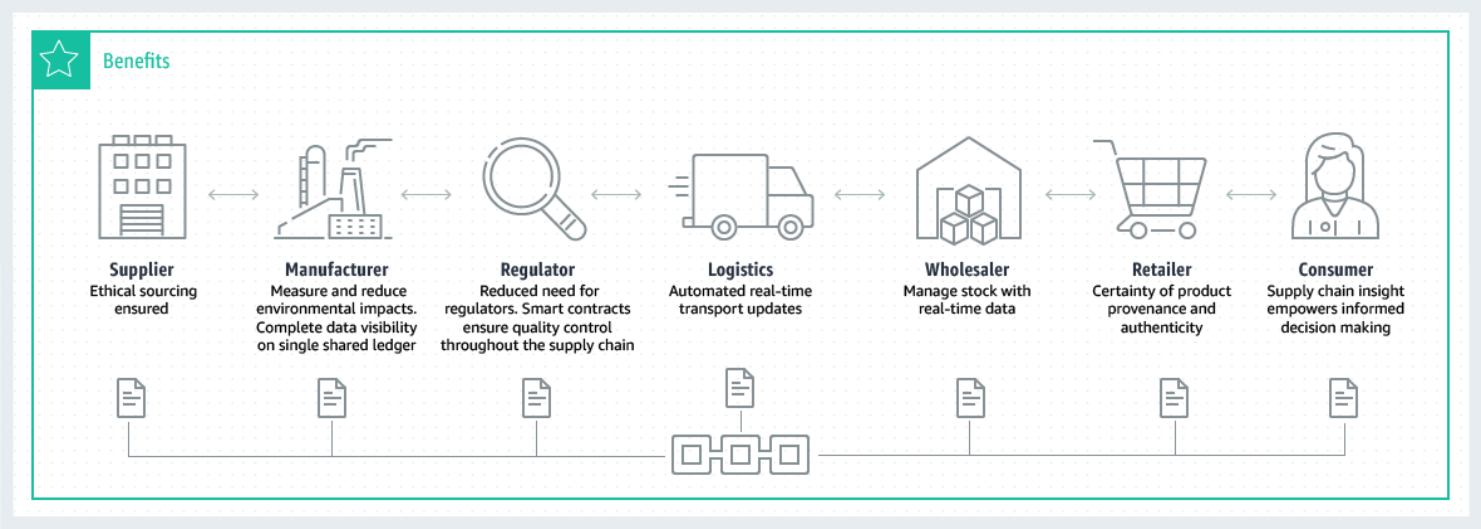
Πηγή: https://aws.amazon.com/blockchain/blockchain-for-supply-chain-track-and-trace/

Καθώς αναπτύσσεται συνεχώς ο τομέας των Logistics, ολοένα και περισσότερες νέες οντότητες, όπως εταιρείες ή οργανισμοί, εμπλέκονται είτε άμεσα είτε έμμεσα στην εφοδιαστική αλυσίδα, οδηγώντας σε μία διαρκώς αυξανόμενη πολυπλοκότητα που δημιουργεί αμφιβολίες όσον αφορά την αξιόπιστη επικοινωνία και διαφάνειά τους.

[34] Πηγή: https://www.econstor.eu/bitstream/10419/209299/1/hicl-2017-23-003.pdf

Η τεχνολογία Blockchain καλείται να αντιμετωπίσει αποτελεσματικά τις παραπάνω προκλήσεις. [36]

Εικόνα 17: Οφέλη εφαρμογής τεχνολογίας Blockchain στον τομέα των Logistics



Πηγή: https://aws.amazon.com/blockchain/blockchain-for-supply-chain-track-and-trace/

2.2 Ερευνητική προσέγγιση

Στο παρόν κεφάλαιο, για την όσο το δυνατόν ευρύτερη και αποδοτικότερη αξιολόγηση της έρευνας της τεχνολογίας Blockchain στα Logistics, αξιοποιήθηκαν στοιχεία που αντλήθηκαν τόσο από ειδησεογραφικές – ενημερωτικές – τεχνολογικές ιστοσελίδες ώστε να εντοπίσουμε σε τι επίπεδο βρισκόμαστε σήμερα, όσο και από σχετικές επιστημονικές δημοσιεύσεις κι άρθρα, βλέπε βιβλιομετρική ανάλυση παρακάτω. Εν συνεχεία, παρουσιάζονται εφαρμογές της Blockchain στην αγορά στους τομείς της εφοδιαστικής αλυσίδας και των Logistics, ενώ αναλύεται εις βάθος το παράδειγμα της IBM όσον αφορά τα τρόφιμα. Τέλος, αξιολογείται η συμφωνία των πρακτικών εφαρμογών με τις ερευνητικές προσδοκίες επί του θέματος.

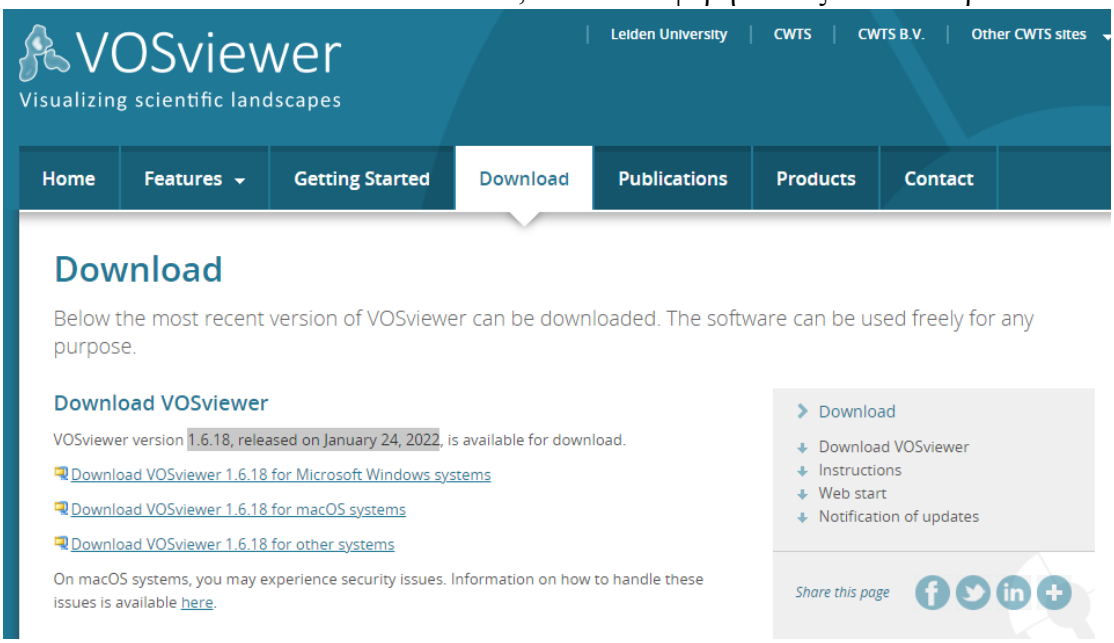
2.3 Βιβλιομετρική Ανάλυση

Όσον αφορά τη μεθοδολογία της βιβλιογραφικής έρευνας, σε συνέχεια του προηγουμένου κεφαλαίου, ακολουθήθηκε η ίδια τακτική, χρησιμοποιώντας το πρόγραμμα VOSViewer, το εργαλείο που κατασκευάζει κι οπτικοποιεί βιβλιομετρικά δίκτυα, ανάλογα των δεδομένων που παρατίθενται. Τα συγκεκριμένα δίκτυα δύνανται επί παραδείγματι να περιλαμβάνουν επιστημονικά περιοδικά, ερευνητές ή μεμονωμένες δημοσιεύσεις και κατασκευάζονται βάσει παραπομπών, βιβλιογραφικής σύζευξης, συν-παραπομπής ή σχέσεων συν-συγγραφικής. Προσφέρεται συν τοις άλλοις λειτουργία εξόρυξης κειμένου η οποία δύναται να χρησιμοποιηθεί για την δημιουργία και την οπτικοποίηση δικτύων συν-εμφάνισης σημαντικών όρων οι οποίοι εξάγονται από το σύνολο της ακαδημαϊκής βιβλιογραφίας.[37]

[35] Πηγή: https://www.newmoney.gr/roh/palmos-oikonomias/oikonomia/ebrd-i-ellada-bori-na-ofelithi-apo-tin-apopagkosmiopiisi/
[36] Πηγή: https://www.pwc.de/de/strategie-organisation-prozesse-systeme/blockchain-in-logistics.pdf, σελίδα 4
[37] Πηγή: https://www.vosviewer.com/

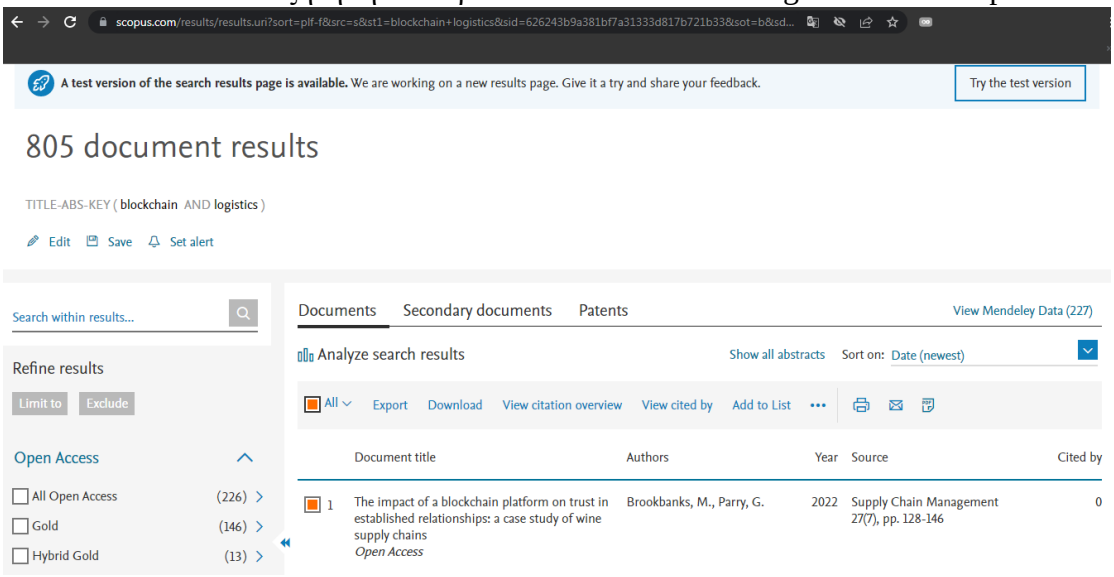
Συγκεκριμένα, στο 2ο κεφάλαιο, τα δεδομένα που χρησιμοποιήθηκαν για την οπτικοποίηση των συγγραφέων με πάνω από 5 δημοσιεύσεις στους τομείς των Blockchain και Logistics καθώς επίσης και των συγγραφέων με περισσότερες αναφορές, αντλήθηκαν από τη βιβλιογραφική βάση δεδομένων της Scopus.com, στην οποία περιλαμβάνονται παραπομπές και περιλήψεις για επιστημονικά άρθρα από έγκριτα ακαδημαϊκά περιοδικά. Στην Scopus αποκτήθηκε πρόσβαση με το λογαριασμό του Πανεπιστημίου Πειραιώς.

Εικόνα 18: VOSViewerVersion 1.6.18, που κυκλοφόρησε στις 24 Ιανουαρίου 2022



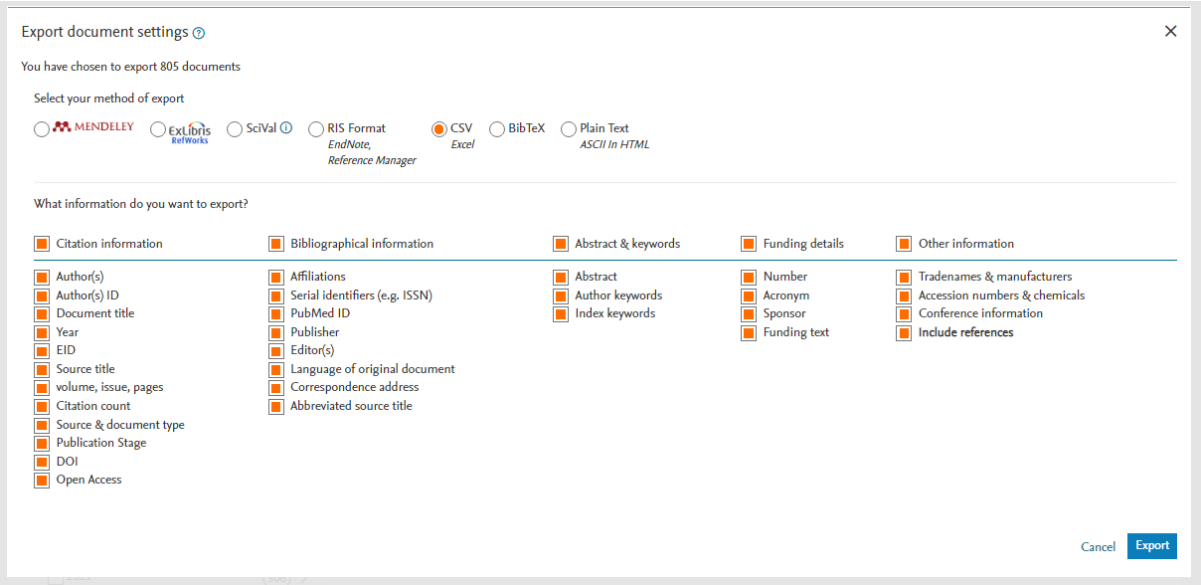
Πηγή: https://www.vosviewer.com/download

Εικόνα 19: Αναζήτηση των όρων "blockchain" και "logistics" στο Scopus



Πηγή: https://www.scopus.com/results/results.uri?sort=plf-f&src=s&st1=blockchain+logistics&sid=626243b9a381bf7a31333d817b721b33&sot=b&sdt=b&sl=35&s=TITLE-ABS-KEY%28blockchain+logistics%29&origin=searchbasic&editSaveSearch=&yearFrom=Before+1960&yearTo=Present

Εικόνα 20: Εξαγωγή σε .csv αρχείο των 805 αρχείων που περιέχουν τους όρους Blockchain, Logistics

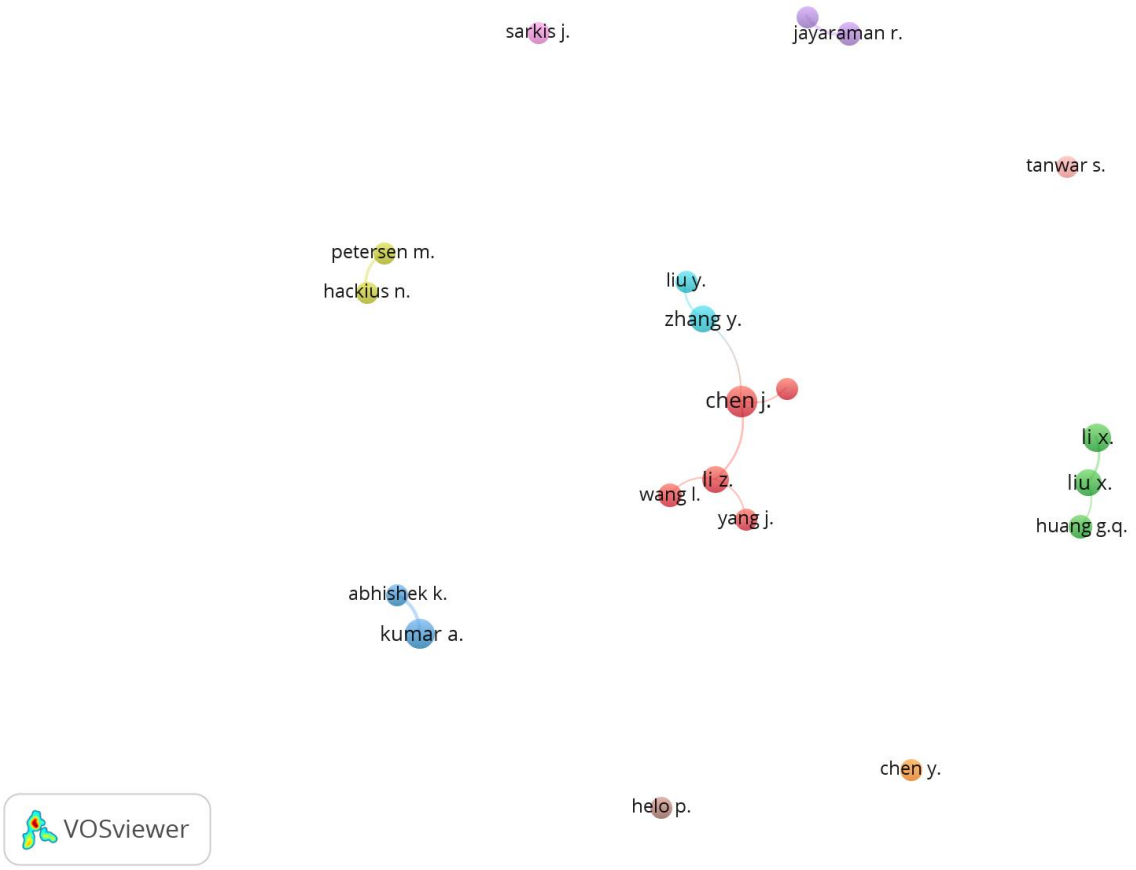


Πηγή: https://www.scopus.com/

Στη συνέχεια εκκινήθη το VOSviewer και επελέχθησαν: Create… → Create a map based on bibliographic data → Read data from bibliographic database files → Scopus →Επιλογή του παραπάνω .csv αρχείου.

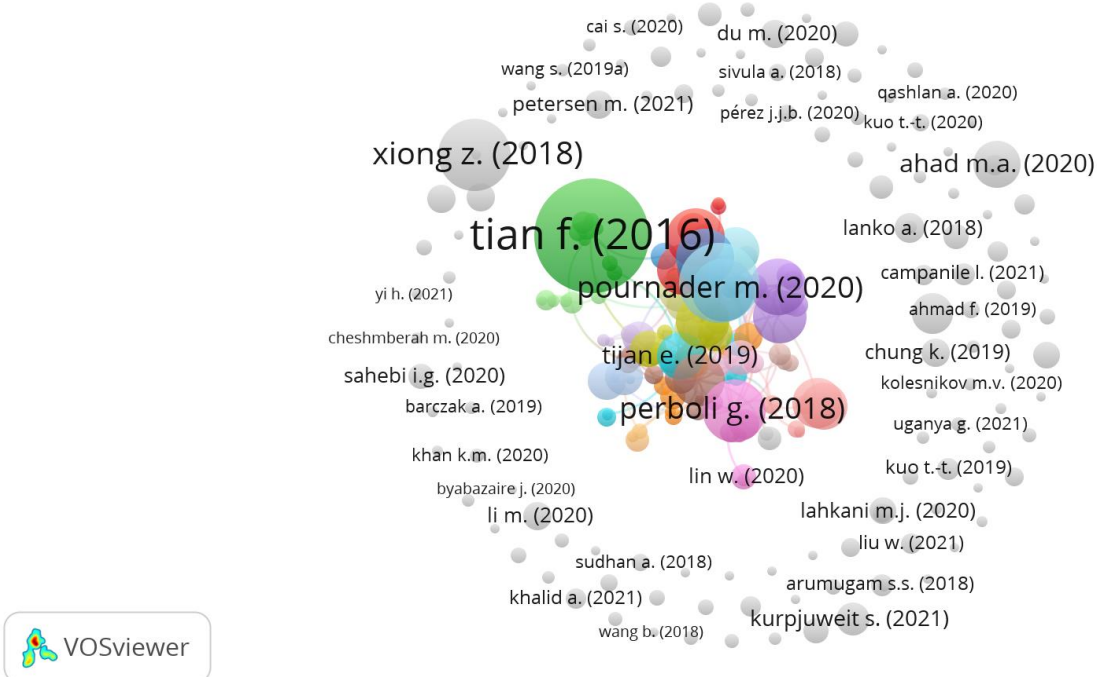
Υπάρχει μία πληθώρα επιλογών για το τι δεδομένα δύνανται να οπτικοποιηθούν. Σε πρώτη φάση, επελέγησαν οι συγγραφείς με πάνω από 5 δημοσιεύσεις στους τομείς Blockchain και Logistics ώστε να φανεί η αλληλεπίδρασή τους (Εικόνα 21).

Εικόνα 21: Οπτικοποίηση συγγραφέων με πάνω από 5 δημοσιεύσεις



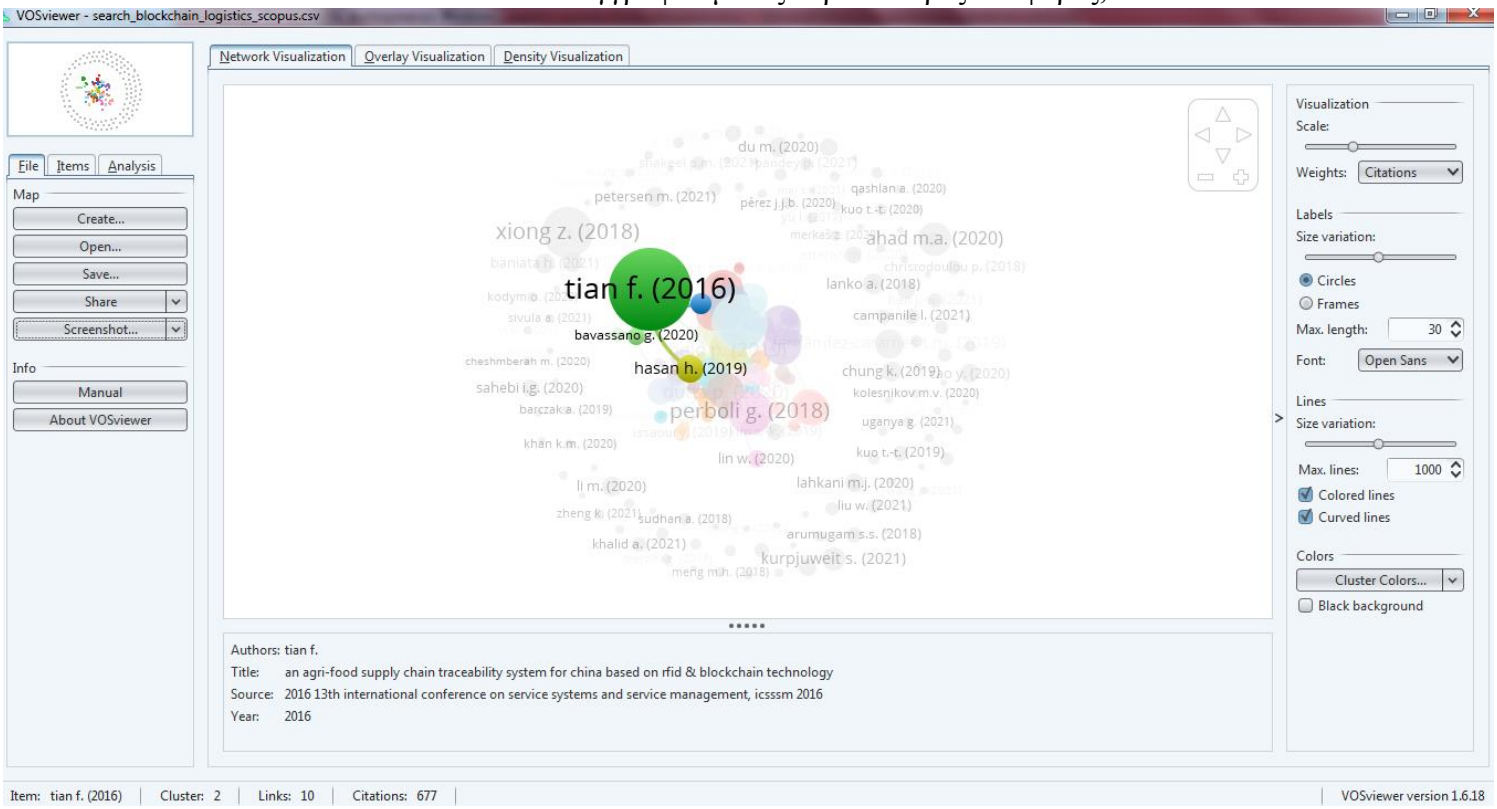
Σε δεύτερη φάση, επελέγη η οπτικοποίηση των συγγραφέων που έχουν τις περισσότερες αναφορές (Εικόνα 22).

Εικόνα 22: Οπτικοποίηση συγγραφέων με περισσότερες αναφορές



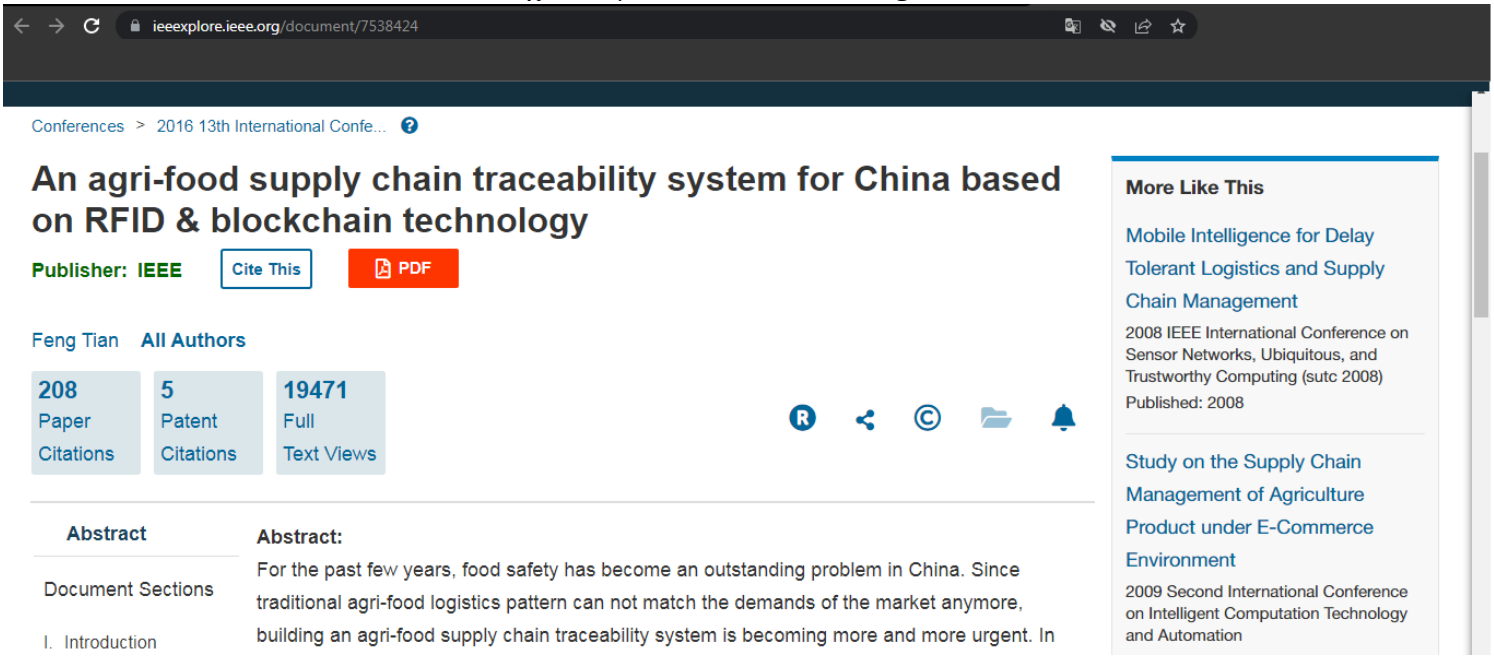
Μάλιστα, παρέχεται η δυνατότητα επιλογής με κλικ οπουδήποτε στο σχήμα για περισσότερες πληροφορίες για το έργο του συγγραφέα. Χαρακτηριστικά, κάνοντας mouseover (μετακίνηση κέρσορα) στον tian f. (2016) βλέπουμε στο VOSviewer το άρθρο του (Εικόνα 23).

Εικόνα 23: Mouseover στον συγγραφέα με τις περισσότερες αναφορές, tian f.



Ακολούθως, μετά το mouseover, αν επιλεχθεί με κλικ ο συγγραφέας στο VOSviewer, μεταβαίνουμε στην ιστοσελίδα όπου υπάρχει η αντίστοιχη δημοσίευσή του (Εικόνα 24).

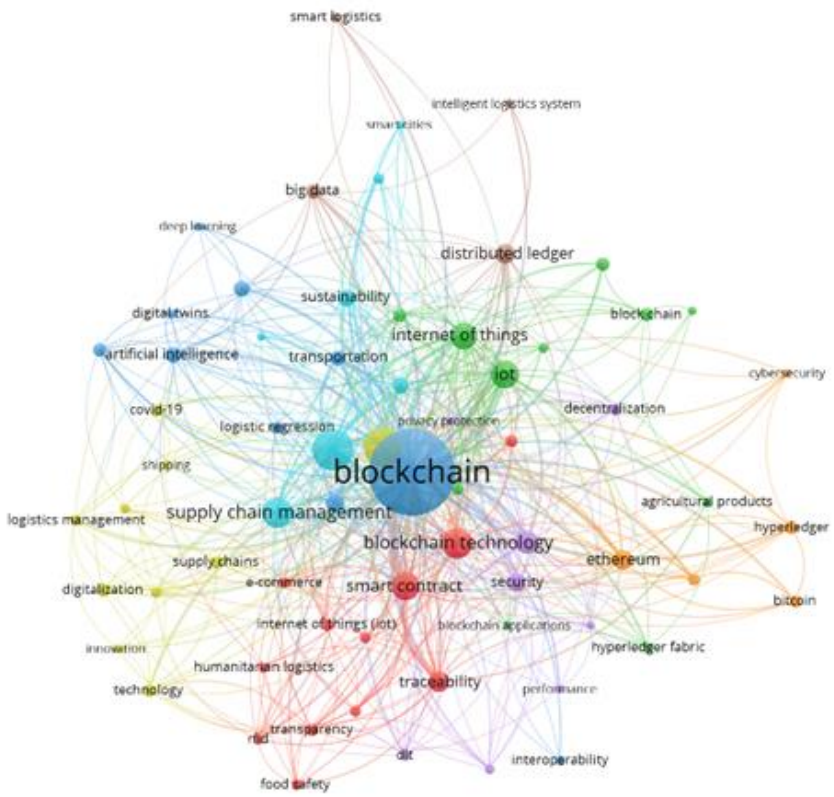
Εικόνα 24: Μετάβαση στο επιστημονικό άρθρο με τις περισσότερες αναφορές σχετικά με Blockchain και Logistics.



Πηγή: https://ieeexplore.ieee.org/document/7538424

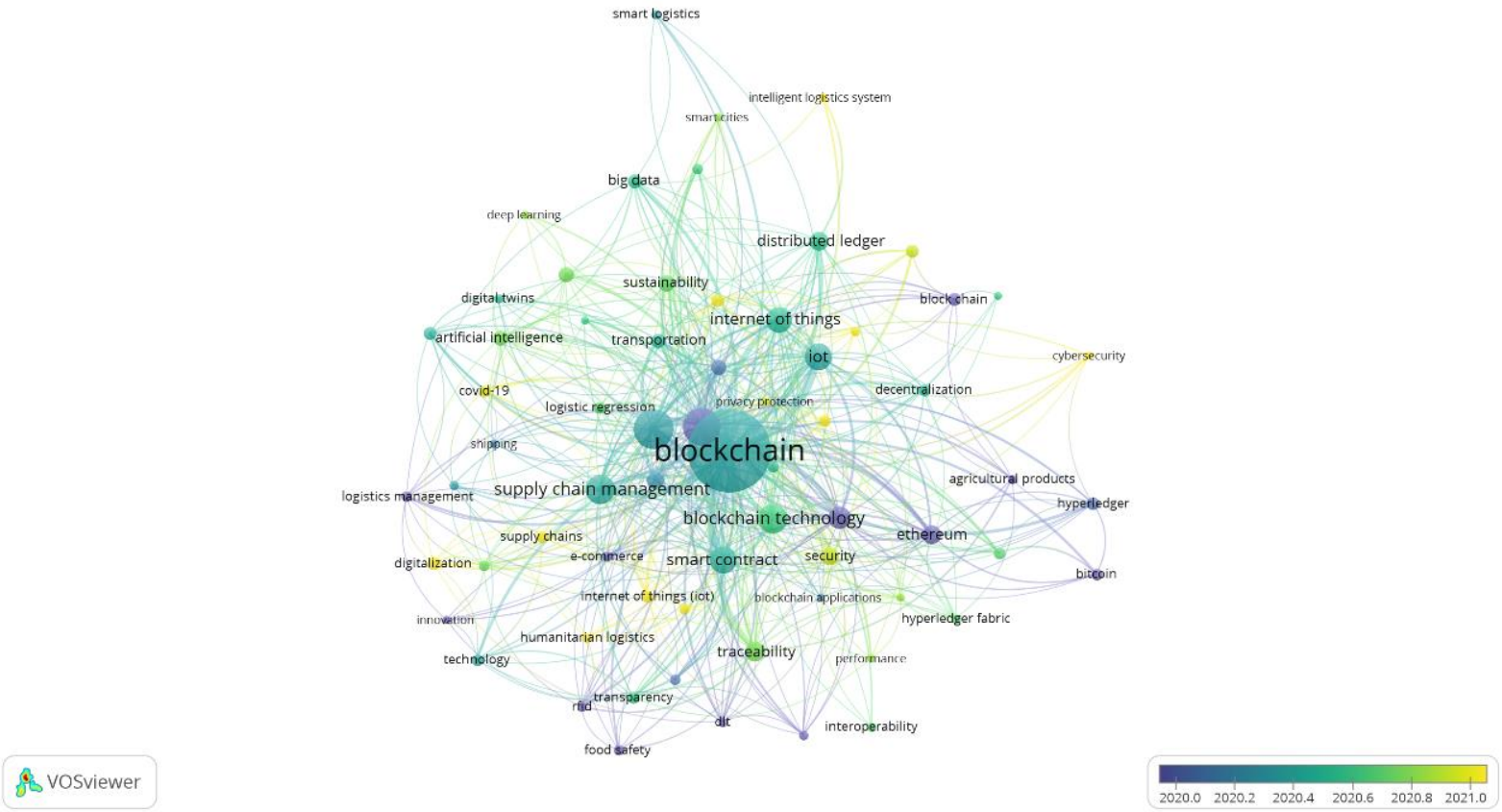
Όπως προαναφέρθηκε, εισήχθησαν τα αποτελέσματα από την αναζήτηση στο scopus.com στο λογισμικό VOSviewer προκειμένου να αναλυθούν οι λέξεις κλειδιά. Από τις 1672 οι 67 όροι αποκρινόντουσαν στα κριτήρια αναζήτησης, σύμφωνα με το VOSviewer. Στην απεικόνιση **Network_Visualization** οι πιο «δυνατοί» όροι αμέσως μετά τον όρο «blockchain» ήταν οι «logistics», «supplychain», «blockchaintechnology», «internetofthings» και «smartcontracts» (Εικόνα 25).

Εικόνα 25: VOSviewer: Network_Visualization



Στην απεικόνιση **Overlay_Visualization** εμφανίζεται η διασπορά των όρων στη διάσταση του χρόνου. Οι νεότεροι όροι και λέξεις – κλειδιά εμφανίζονται με διαφορετικό χρωματισμό. Πιο συγκεκριμένα, με πιο κίτρινο χρώμα είναι οι πιο πρόσφατες δημοσιεύσεις, όποτε σε αυτές παρουσιάζονται όροι και λέξεις – κλειδιά όπως «cybersecurity», «cloud computing», «internet of things», «covid-19» και πολύ περισσότερο «edge computing» και «reverse logistics». Η έρευνα δείχνει να προσανατολίζεται προς το Cybersecurity και το Edge Computing, ενώ ενδιαφέρον δείχνει και το Reverse Logistics. Φυσικά, λόγω της πανδημίας, η έρευνα γύρω από τις συνέπειες του Covid-19 και τα Logistics δείχνει να προσελκύει και αυτή με τη σειρά της έντονο ερευνητικό ενδιαφέρον. Στην παρακάτω εικόνα φαίνεται η διασπορά των δημοσιεύσεων στη διάσταση του χρόνου. Αξιοσημείωτο είναι ότι στη συγκεκριμένη εικόνα λόγω ρύθμισης παραμέτρων, το VOSviewer δείχνει τα δημοσιεύματα μεταξύ των ετών 2020 και εφεξής.

Εικόνα 26: VOSviewer: Overlay_Visualization

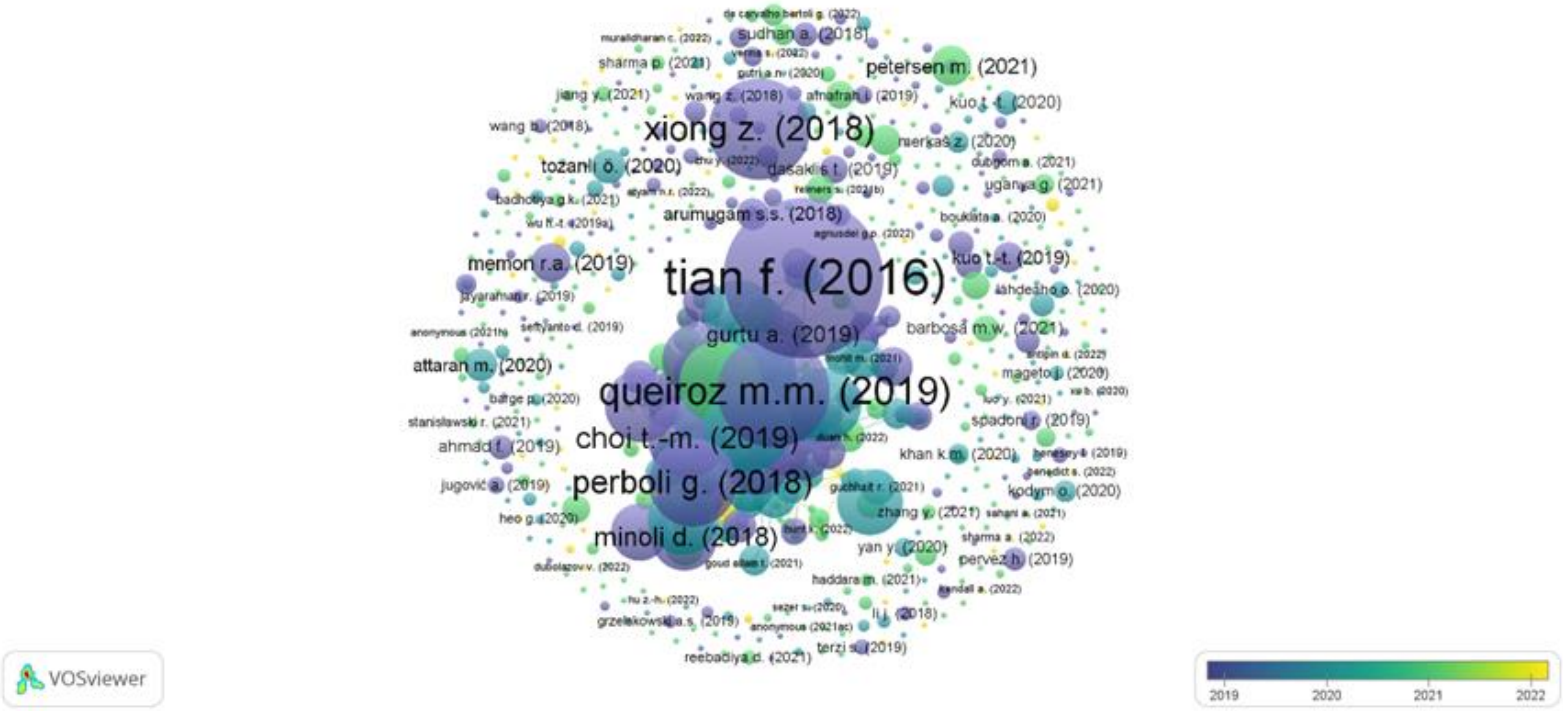


Σε συνέχεια της παρούσας βιβλιομετρικής ανάλυσης, στα παρακάτω στιγμιότυπα παρατηρείται η δυνατότητα απόκτησης αναφορών στη διάσταση του χρόνου για την κάθε δημοσίευση με το συγκεκριμένο συγγραφέα μαζί με τον συνολικό αριθμό των παραπομπών από άλλες εργασίες προς τη συγκεκριμένη δημοσίευση. Αυτό μπορεί να γίνει τόσο για τη βιβλιογραφική ζεύξη (bibliographic coupling), όσο και για την συν – παραπομπή (co-citation).

Εικόνα 27: VOSviewer: Στιγμιότυπο από πίνακα δημοσιεύσεων ανά χρονιά, ανά συγγραφέα και σύνολο παραπομπών προς τη συγκεκριμένη δημοσίευση.

Selected	Document	Citations	Links
☑	queiroz m.m. (2019)	330	33
☑	tijan e. (2019)	116	33
☑	perboli g. (2018)	205	33
☑	dutta p. (2020)	140	28
☑	pournader m. (2020)	204	22
☑	helo p. (2019)	147	22
☑	karakas s. (2021)	2	21
☑	chang s.e. (2020a)	63	19
☑	koh l. (2020)	56	17
☑	choi t.-m. (2019)	166	17
☑	tian f. (2016)	677	17
☑	dutta p. (2022)	0	16
☑	hasan h. (2019)	68	16
☑	xu x. (2022)	1	12
☑	dolgui a. (2020)	174	12
☑	samad t.a. (2022)	0	11
☑	helo p. (2020)	64	11
☑	chang y. (2020)	131	11
☑	tang c.s. (2019)	144	11
☑	choi t.-m. (2022)	1	10
☑	astarita v. (2020)	52	10

Εικόνα 28: VOSviewer: Οπτικοποιημένα δεδομένα του παραπάνω πίνακα.



Τέλος, αναφορικά με τη βιβλιομετρική ανάλυση, παρέχεται και η δυνατότητα εμφάνισης της διασποράς των δημοσιευμάτων ανά χώρα, όπως φαίνεται στον παρακάτω πίνακα. Από το συγκεκριμένο πίνακα καθίσταται εμφανές ότι οι χώρες με τις περισσότερες δημοσιεύσεις είναι κατά σειρά η Κίνα, η Ινδία, οι ΗΠΑ κ.ο.κ.

Εικόνα 29: VOSviewer: Στιγμιότυπο από πίνακα δημοσιεύσεων ανά χώρα.

Selected	Country	Documents	Citations	Total link strength
☑	china	188	1576	66
☑	india	103	851	53
☑	united states	70	1644	56
☑	russian federation	45	353	19
☑	germany	40	801	22
☑	united kingdom	36	601	36
☑	italy	32	525	18
☑	australia	28	535	39
☑	taiwan	25	345	27
☑	south korea	24	207	19
☑	hong kong	23	606	17
☑	france	21	709	20
☑	spain	18	227	11
☑	united arab emirates	18	199	11
☑	turkey	18	138	9
☑	saudi arabia	18	111	33
☑	finland	16	365	12
☑	canada	15	312	24
☑	malaysia	15	135	18
☑	sweden	14	173	10

2.4 Ορισμός της Blockchain

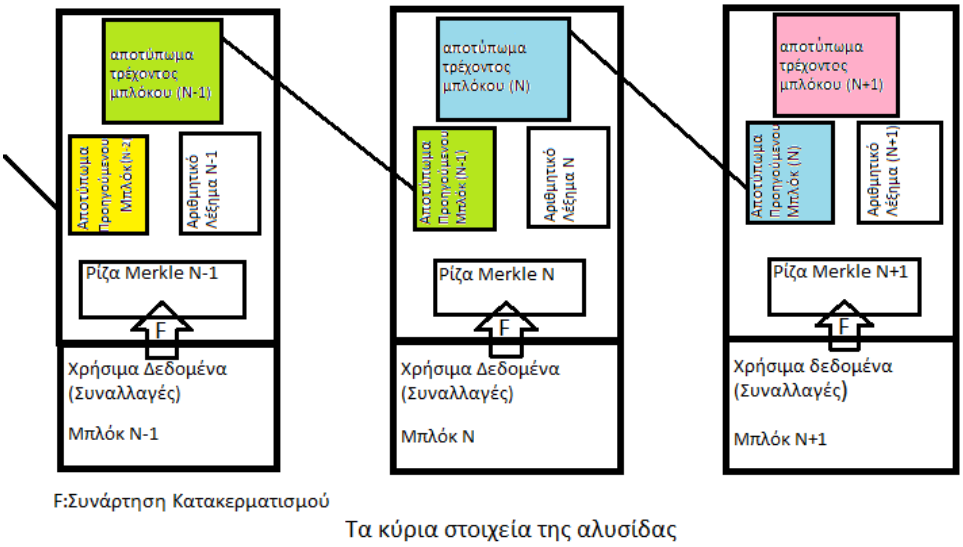
Ουσιαστικά η Blockchain είναι μία μαθηματική δομή για την αποθήκευση ψηφιακών συναλλαγών ή δεδομένων σε ένα αμετάβλητο, κατανεμημένο, αποκεντρωμένο ψηφιακό λογιστικό βιβλίο (βάση δεδομένων) που αποτελείται από μπλοκ που συνδέονται μέσω κρυπτογραφικής υπογραφής που με τα σημερινά δεδομένα είναι σχεδόν αδύνατο να πλαστογραφηθεί, να παραβιαστεί ή να διακοπεί.[38]

Πρόκειται δηλαδή για μια ψηφιακή αλυσίδα από blocks δεδομένων. Έχει σχεδιαστεί με τέτοιο τρόπο ώστε κάθε μπλοκ, ή κρίκος στην αλυσίδα, να συνδέεται περίπλοκα με το προηγούμενο μπλοκ μέσω κρυπτογραφικών μεθόδων. Αυτό σημαίνει ότι εάν κάποιος επιχειρήσει να αλλάξει ένα μπλοκ στη μέση της αλυσίδας, θα πρέπει να τροποποιήσει όλα τα επόμενα μπλοκ για να παραμείνει έγκυρη η Blockchain. Εάν δεν γίνει αυτό, όλα τα μπλοκ μετά το τροποποιημένο καθίστανται άκυρα. Η Blockchain αποτελείται από μπλοκ που περιέχουν διάφορους τύπους δεδομένων και δεν περιορίζονται αποκλειστικά για οικονομικές συναλλαγές. Αυτά τα μπλοκ χρησιμεύουν για την ασφαλή καταγραφή και διατήρηση τυχόν επιθυμητών δεδομένων χωρίς τον κίνδυνο αλλοίωσης.[39] Γι' αυτό το λόγο θεωρείται πρωτόκολλο κυβερνοασφάλειας του μέλλοντος.

[38] Πηγή: https://connect.comptia.org/content/articles/blockchain-terminology

[39] Πηγή: https://www.pcsteps.gr/214154-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7-blockchain-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82/

Εικόνα 30: Δομή Blockchain



Τα κύρια στοιχεία της αλυσίδας

Πηγή: https://upload.wikimedia.org/wikipedia/commons/8/8b/%CE%91%CE%BB%CF%85%CF%83%CE%AF%CE%B4%CE%B1_%CE%9A%CE%BF%CE%B9%CE%BD%CE%BF%CF%80%CE%BF%CE%B9%CE%AE%CF%83%CE%B5%CF%89%CE%BD_2.png

2.5 Παράδειγμα Blockchain σε υπηρεσίες Logistics

Εικόνα 31: Διαφάνεια στην Εφοδιαστική Αλυσίδα και διαδικασίες βάσει δεδομένων

Πηγή: https://www.fleetboard.info/news/blockchain-ecosystem/#/

Η εταιρεία Fleetboard που δραστηριοποιείται στον χώρο των Logistics σε συνεργασία με την Imperial Logistics International, υιοθετώντας το πρωτόκολλο Blockchain, σύμφωνα με το παραπάνω σχήμα έχει ορίσει τη διαδικασία ως εξής.

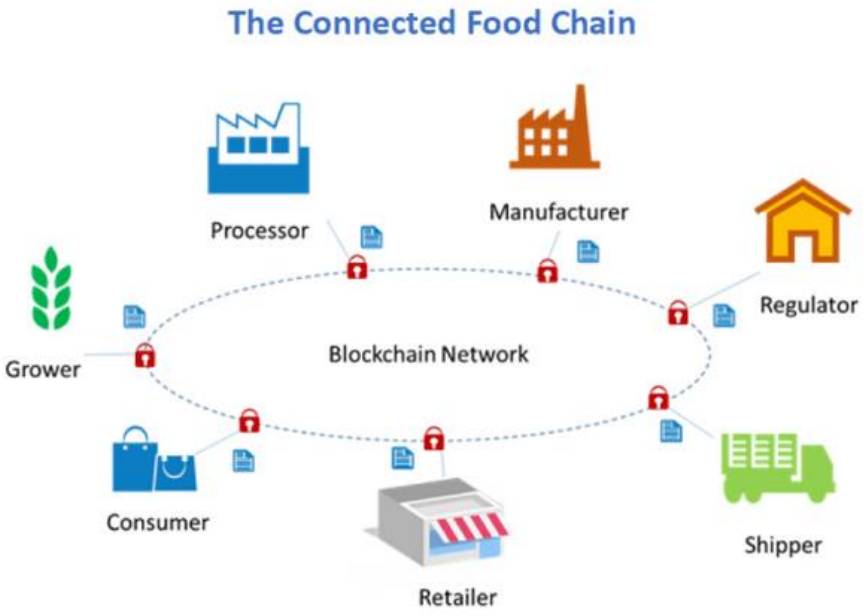
Στο πρώτο βήμα, δύο ή περισσότερα μέρη συμφωνούν για την ποιότητα της υπηρεσίας και τις απαιτήσεις χρόνου της παράδοσης. Ενώ το φορτηγό είναι καθ' οδόν, η Fleetboard θα παρακολουθεί δεδομένα κατάστασης φόρτωσης ή συμβάντα,

όπως ανωμαλίες στη θερμοκρασία κατά τη μεταφορά ιατρικών προϊόντων και θα γράφει τα αποτελέσματα στη Blockchain. Μόλις φτάσει το φορτηγό, τα δεδομένα μπορούν να χρησιμοποιηθούν για την επικύρωση της σύμβασης. Ανάλογα με τις συμφωνίες, ενεργοποιείται αυτόματα ο διακανονισμός υπό όρους. Για παράδειγμα, εάν η θερμοκρασία και ο χρόνος ήταν εντάξει, θα μπορούσε να ενεργοποιηθεί μια άμεση πληρωμή, αυτόματη τιμολόγηση και θετική βαθμολογία.

Ένα τέτοιο σύστημα αξιολόγησης σε συνδυασμό με την άμεση πληρωμή είναι μια πραγματική αλλαγή του παιχνιδιού για την αγορά Logistics. Η επιλογή ενός παρόχου Logistics δεν θα βασίζεται αποκλειστικά στην ικανότητα λήψης χαμηλών περιθωρίων κέρδους και μεγάλης περιόδου πληρωμής, αλλά μάλλον και στην ποιότητα της υπηρεσίας.[40]

2.6 Παράδειγμα Blockchain στην εφοδιαστική αλυσίδα στην βιομηχανία τροφίμων

Εικόνα 32: Blockchainin Food Chain



Πηγή: https://www.pcsteps.gr/wp-content/uploads/2100/07/Blockchain_3aaa.png

Στον τομέα της βιομηχανίας των τροφίμων, η Blockchain έχει τη δυνατότητα να καταγράφει ολοκληρωμένες πληροφορίες σχετικά με τον ακριβή προορισμό ενός προϊόντος, που εκτείνεται από την παραγωγή έως τη λιανική του πώληση. Αυτό περιλαμβάνει λεπτομέρειες όπως φερειπείν την τοποθεσία και την ημερομηνία σφαγής των ζώων, την επεξεργασία του κρέατος, τα στάδια της μεταφοράς, τις συνθήκες ψύξης, τις πληροφορίες του κρεοπωλείου και την ακριβή ώρα πώλησης. Στην περίπτωση της μόλυνσης από επιβλαβείς μικροοργανισμούς, βάσει των πληροφοριών της Blockchain, δύναται ο άμεσος και ακριβής εντοπισμός της πηγής ώστε να αναγνωριστούν και τα άλλα κρέατα από την ίδια παρτίδα.[39]

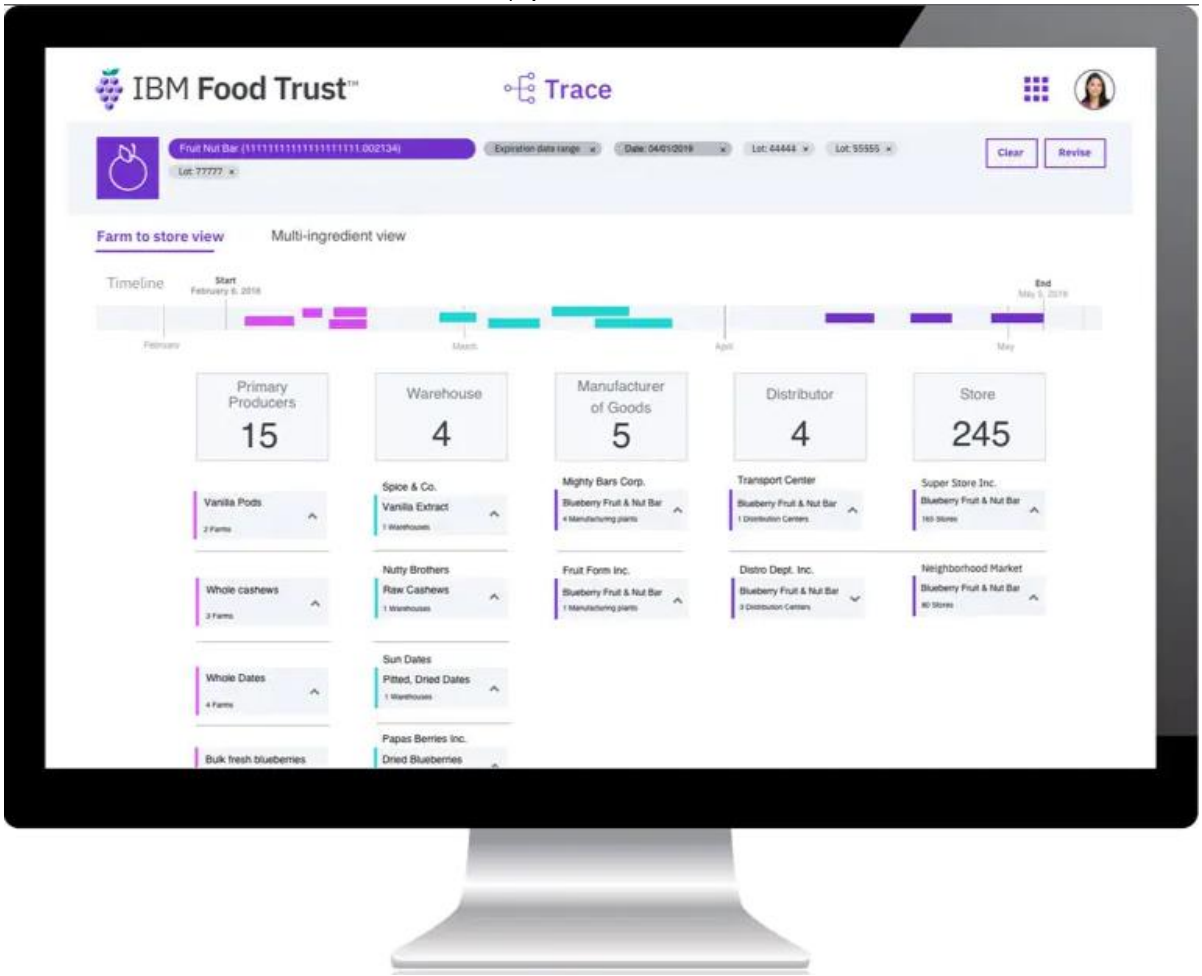
[40] Πηγή: https://www.fleetboard.info/news/blockchain-ecosystem/#/

Η IBM αναπτύσσει επί του παρόντος το σύστημα Blockchain Food Trust™ για το σκοπό αυτό.

2.7 Το σύστημα τεχνολογίας Blockchain Food Trust™ της IBM

Το IBM Food Trust™ είναι ένα συνεργατικό δίκτυο καλλιεργητών, μεταποιητών, χονδρεμπόρων, διανομέων, κατασκευαστών, λιανοπωλητών και άλλων, το οποίο ενισχύει την διαφάνεια και την υπευθυνότητα σε όλη την αλυσίδα εφοδιασμού τροφίμων. Χτισμένη στην IBM Blockchain, αυτή η λύση συνδέει τους συμμετέχοντες μέσω ενός εγκεκριμένου, αμετάβλητου και κοινόχρηστου αρχείου προέλευσης των τροφίμων, δεδομένων συναλλαγών, λεπτομερειών επεξεργασίας και άλλων.[41]

Εικόνα 33: Διεπαφή του IBM Food Trust™



Πηγή: https://www.ibm.com/uk-en/blockchain/solutions/food-trust/modules

Τα οφέλη από τη χρήση της είναι τα εξής[42] :

2.7.1 Αποτελεσματικότητα της Εφοδιαστικής Αλυσίδας

Η αναποτελεσματικότητα του συστήματος τροφίμων είναι ένα διάχυτο πρόβλημα παγκοσμίως, το οποίο έγινε πιο εμφανές από την κρίση του COVID-19, η

[41] Πηγή: https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust

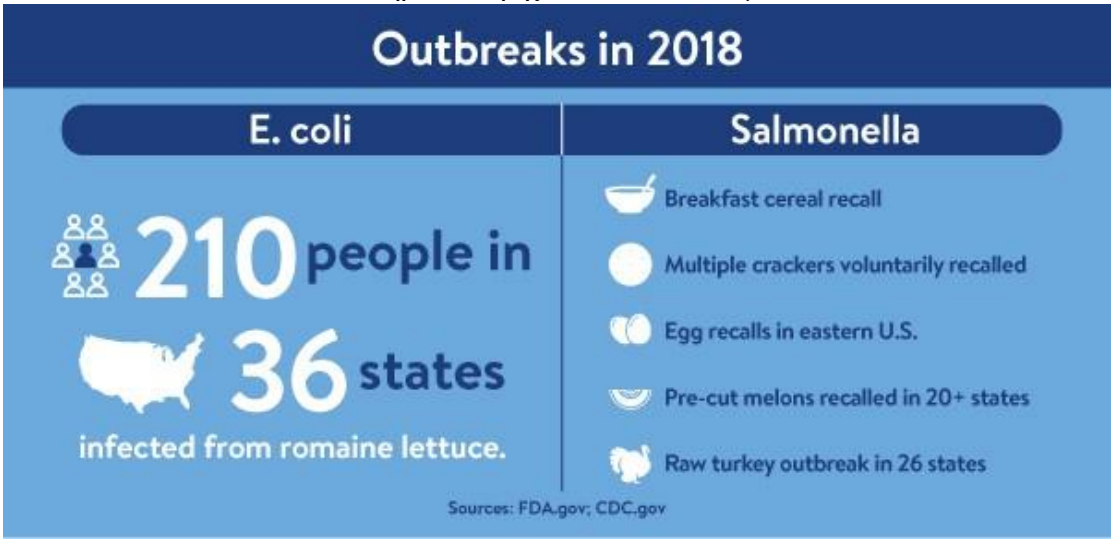
[42] Πηγή: https://www.ibm.com/blockchain/resources/7-benefits-ibm-food-trust/

οποία διατάραξε την παγκόσμια αλυσίδα εφοδιασμού. Με τόσους πολλούς συμμετέχοντες, υπάρχουν αρκετές πιθανότητες για απώλεια της αποτελεσματικότητας και των κερδών. Οι αναποτελεσματικότητες επηρεάζουν αρνητικά την τιμολόγηση των καταναλωτών, το αποτύπωμα άνθρακα, τη σπατάλη τροφίμων και την αναμενόμενη φρεσκάδα. Σύμφωνα με τα Ηνωμένα Έθνη, 1,4 δισεκατομμύρια τόνοι ευπαθών τροφίμων χάνονται λόγω ανεπάρκειας που διαπιστώθηκε στην αλυσίδα εφοδιασμού τροφίμων.[43]

Μια κοινή ψηφιακή αλυσίδα εφοδιασμού τροφίμων που τροφοδοτείται από την Blockchain βοηθά τους εμπλεκόμενους παράγοντες της εφοδιαστικής αλυσίδας να συνεργάζονται καλύτερα μεταξύ τους για να λειτουργούν πιο αποτελεσματικά και να προσαρμόζονται σε αλλαγές.

Η πιο έξυπνη εργασία σε ένα κοινό οικοσύστημα οδηγεί στον εύκολο εντοπισμό των αναποτελεσματικών διαδικασιών, την εξάλειψη των σημείων συμφόρησης και την βελτιστοποίηση της αλυσίδας εφοδιασμού για συνεχή ανάπτυξη.

Εικόνα 34: Βακτήρια Εσεριχία Κόλι και Σαλμονέλα το 2018



Πηγή: https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens

2.7.2 Εμπιστοσύνη της επωνυμίας (Brand trust)

Τώρα περισσότερο από ποτέ, οι καταναλωτές έχουν πολλές επιλογές όσον αφορά το πού να αγοράσουν το φαγητό τους. Με μια τόσο ανταγωνιστική βιομηχανία τροφίμων, η διαφοροποίηση της επωνυμίας είναι σημαντική για να παραμείνει στην κορυφή των αποφάσεων αγοράς. Η βιωσιμότητα, συχνά ο βασικός παράγοντας διαφοροποίησης σε μια πολυσύχναστη αγορά, είναι σημαντικό κριτήριο όσον αφορά την αφοσίωση των καταναλωτών. Οι τάσεις δείχνουν ότι οι καταναλωτές θέλουν να γνωρίζουν περισσότερα από τις διατροφικές πληροφορίες, όπως φερειπείν, την προέλευση του τροφίμου, πότε καλλιεργήθηκε και πώς.

Με γνώμονα τις πρόσφατες προσπάθειες ευαισθητοποίησης για τη βιωσιμότητα, η προσοχή των καταναλωτών στο θέμα αυξάνεται. Σύμφωνα με σχετική έρευνα της Nielsen, το 78% των ερωτηθέντων ήταν πρόθυμοι να αλλάξουν τις

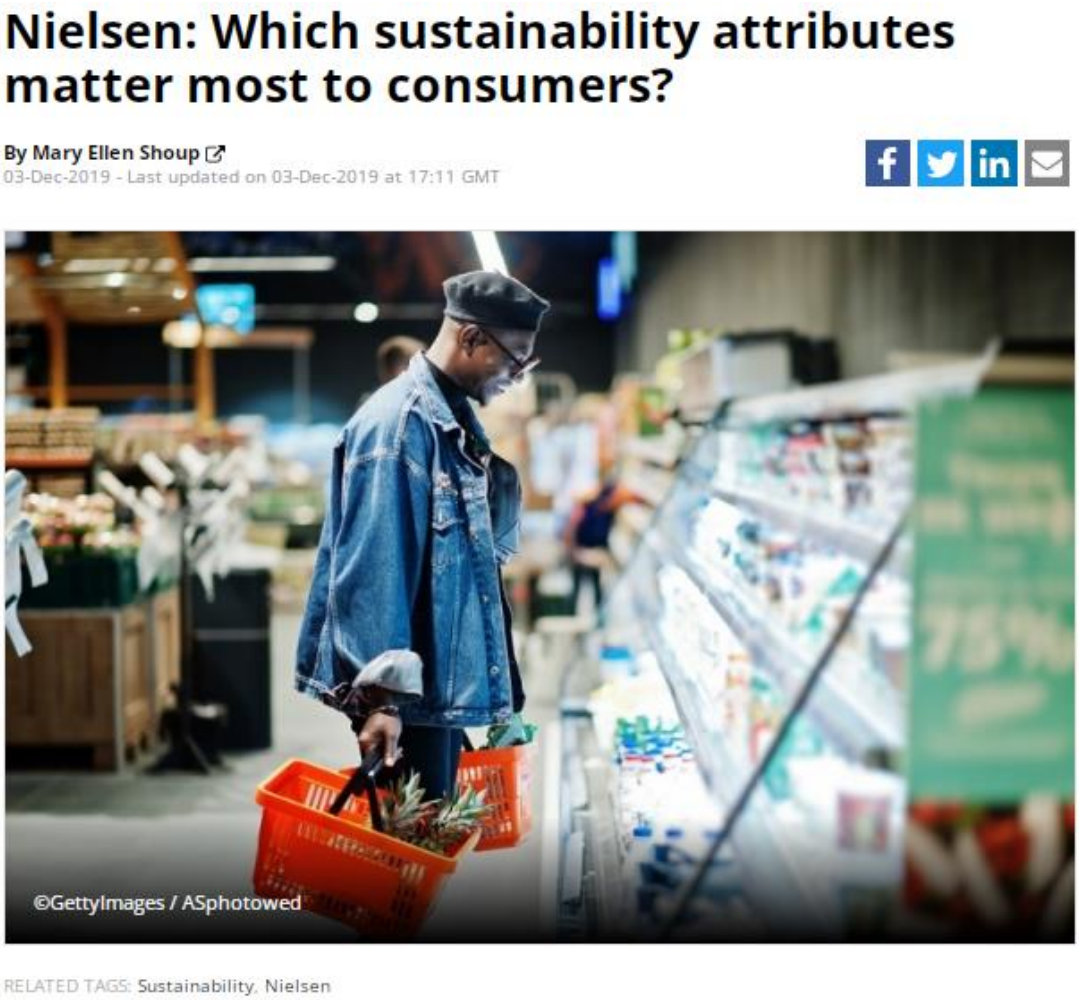
[43] Πηγή: https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens

συνήθειες κατανάλωσης τροφίμων για να μειώσουν τις περιβαλλοντικές τους επιπτώσεις.[44]

Ο πήχης ανεβαίνει και για ασφάλεια και για ποιότητα. Οι εταιρείες τροφίμων θέτουν τα δικά τους ανεξάρτητα πρότυπα και προγράμματα για την ασφάλεια και τη φρεσκάδα των τροφίμων, πέρα από αυτά που απαιτούνται για τη συμμόρφωση.

Επιπλέον, το 20% των αγοραστών άλλαξαν μάρκα μετά από ανάκληση προϊόντος, σύμφωνα με έρευνα του 2019 στο Ηνωμένο Βασίλειο[45]. Οι καταναλωτές, μαζί με άλλους βασικούς παράγοντες στο σύστημα τροφίμων, θέλουν περισσότερες λεπτομέρειες και διαφάνεια σχετικά με τα τρόφιμα που καταναλώνουν, προκειμένου να λαμβάνουν τεκμηριωμένες αποφάσεις.

Εικόνα 35: Αλλαγή συμπεριφοράς του 78 % των καταναλωτών για μείωση περιβαλλοντικών επιπτώσεων



Πηγή: https://www.foodnavigator-usa.com/Article/2019/12/03/Nielsen-Which-sustainability-attributes-matter-most-to-consumers

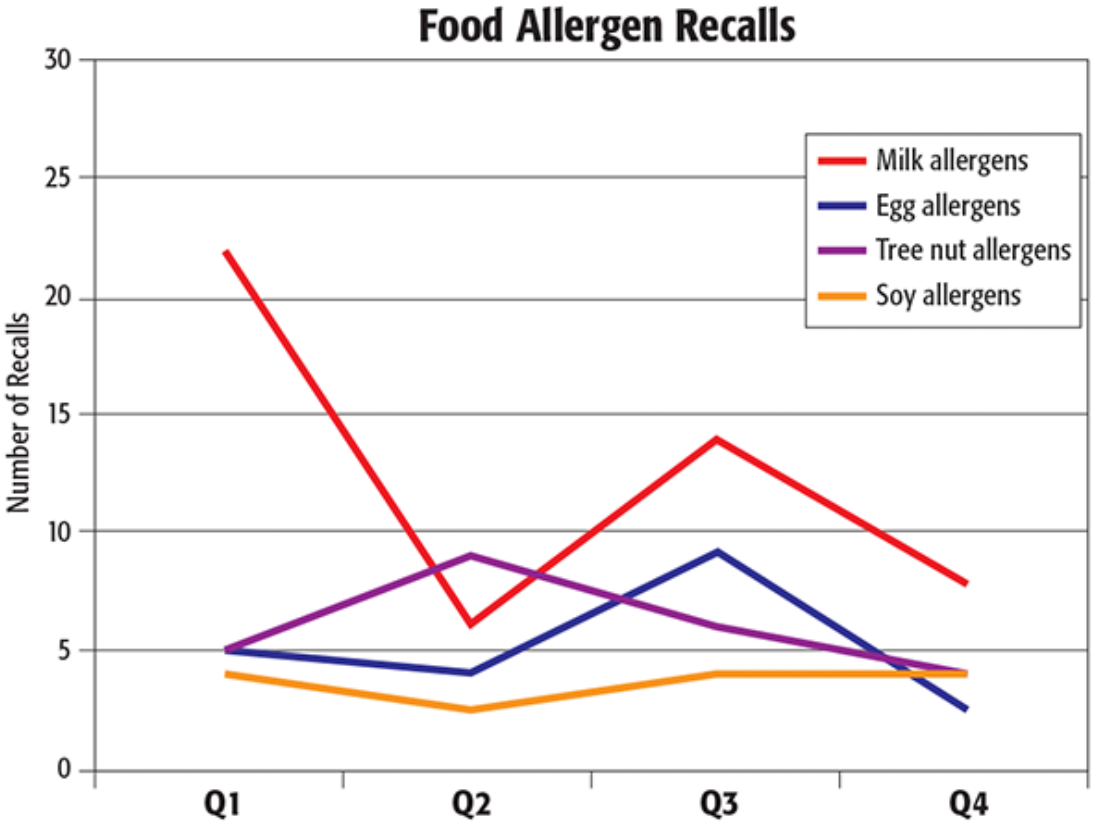
[44] Πηγή: https://www.foodnavigator-usa.com/Article/2019/12/03/Nielsen-Which-sustainability-attributes-matter-most-to-consumers

[45] Πηγή: https://www.lrqa.com/en-gb/resources/2019-uk-food-survey/

2.7.3 Ασφάλεια τροφίμων

Οι ανακλήσεις τροφίμων αποτελούν τεράστιο πρόβλημα ασφάλειας και απειλή για την κερδοφορία. Το 2019, το περιοδικό FoodSafety μέτρησε 337 ανακλήσεις για την ασφάλεια τροφίμων στις ΗΠΑ.[46] Οι εταιρείες που συμμετείχαν στην έρευνα ανέφεραν κόστος έως και 30 εκατομμύρια USD ανά περιστατικό[47], που προέρχεται από άμεσο κόστος συν το έμμεσο κόστος όπως ποινές, αγωγές, χαμένες πωλήσεις και ζημιά επωνυμίας. Εκτός από τον κοινωνικό και επιχειρηματικό αντίκτυπο, τεράστια αποθέματα τροφίμων σπαταλούνται και η εμπιστοσύνη των καταναλωτών συντρίβεται.

Εικόνα 36: Ανακλήσεις φαγητών με μη δηλωμένα αλλεργιογόνα το 2019 στις ΗΠΑ



Πηγή: https://www.food-safety.com/articles/6487-a-look-back-at-2019-food-recalls

Δεν μπορούν όλες οι εταιρείες να εντοπίσουν γρήγορα την αιτία ενός περιστατικού ασφάλειας τροφίμων. Η ανίχνευση τροφίμων σε όλη την αλυσίδα εφοδιασμού διαρκεί μέρες, αν όχι εβδομάδες, καθώς οι εταιρείες αγωνίζονται να παρακολουθήσουν έναν συνδυασμό ψηφιακής και έντυπης τεκμηρίωσης δεδομένων τροφίμων σε ένα περίπλοκο και αναπτυσσόμενο δίκτυο προμηθευτών και διανομέων.

Τα κενά στην παρακολούθηση της εφοδιαστικής αλυσίδας δημιουργούν τρωτά σημεία. Οι ελλείψεις στις διαδικασίες παραγωγής και παρακολούθησης εκθέτουν το σύστημα τροφίμων σε ευπάθειες που θα μπορούσαν να εξαλειφθούν. Σε απάντηση, ορισμένοι έμποροι λιανικής, όπως η Walmart, αναπτύσσουν Blockchain

[46] Πηγή: https://www.food-safety.com/articles/6487-a-look-back-at-2019-food-recalls

[47] Πηγή: https://www.snackandbakery.com/articles/92105-evaluating-the-real-costs-of-a-food-product-recall

για ιχνηλασιμότητα και παρακολούθηση από άκρο σε άκρο των προϊόντων διατροφής στην αλυσίδα εφοδιασμού.[48]

Οι απαρχαιωμένες πρακτικές ιχνηλασιμότητας τροφίμων δεν έχουν κατασκευαστεί για τη σύγχρονη εποχή.

Με ένα ψηφιακό σύστημα τροφίμων, οι συμμετέχοντες στο δίκτυο έχουν πρόσβαση σε εργαλεία και δεδομένα για να βελτιώσουν την ασφάλεια των τροφίμων και να συμβάλουν ενεργά στη βελτίωση του συστήματος τροφίμων στο σύνολό του.

Η τεχνολογία Blockchain αποθηκεύει ψηφιοποιημένα αρχεία με αποκεντρωμένο και αμετάβλητο τρόπο, προάγοντας την εμπιστοσύνη και τη διαφάνεια που με τη σειρά του βοηθά στη βελτίωση του συστήματος τροφίμων και στη διασφάλιση ασφαλέστερων τροφίμων.

Εικόνα 37: Το timeline της εφαρμογής Blockchain από τη Walmart

Πηγή: https://thegemba.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency

2.7.4 Βιωσιμότητα

Σε όλο τον κόσμο, οι καταναλωτές απαιτούν να μάθουν περισσότερα για το φαγητό τους, ήτοι από πού προήλθε, την επίδραση των μεθόδων παραγωγής του στον πλανήτη μας και πώς αντιμετωπίστηκαν οι εργαζόμενοι και τα ζώα στη διαδικασία.

Στην πραγματικότητα, το 54% των καταναλωτών λέει ότι είναι τουλάχιστον κάπως σημαντικό τα τρόφιμα που αγοράζουν να παράγονται με περιβαλλοντικά βιώσιμο τρόπο.[49] Η βιωσιμότητα δεν αποτελεί πλέον μπόνους, είναι επιτακτική ανάγκη τόσο για τους καταναλωτές που το απαιτούν όσο και για μελλοντικά επιχειρηματικά μοντέλα.

Οι καταναλωτές γίνονται πιο συνειδητοποιημένοι για το οικολογικό τους αποτύπωμα όπως παρουσιάζει η έρευνα της Nielsen.[50]

Το «True Cost Accounting» ρίχνει φως στην τιμή των μη βιώσιμων πρακτικών τροφίμων. Η μη βιώσιμη προμήθεια και η απώλεια βιοποικιλότητας, λόγω μη βιώσιμων μεθόδων παραγωγής, έχουν ως αποτέλεσμα κρυφό κόστος. Έρευνες

[48]Πηγή: https://thegemba.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency

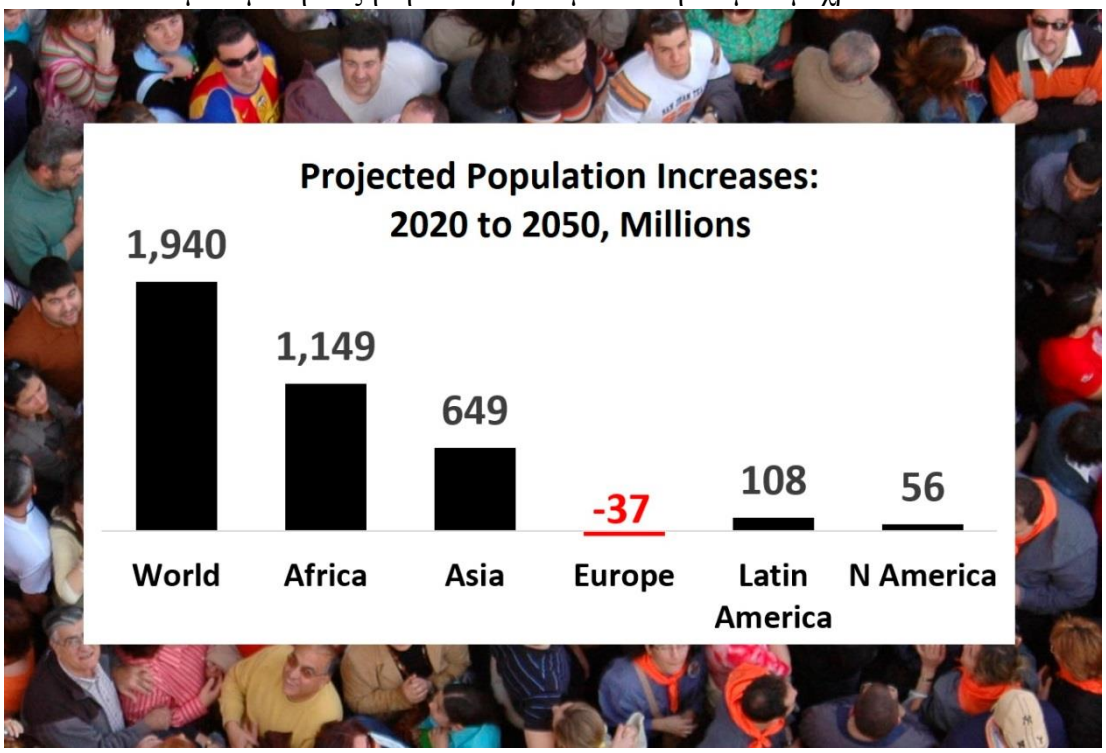
[49]Πηγή: https://foodinsight.org/consumers-insights-future-of-food-sustainability-food-waste/

[50]Πηγή: https://www.foodnavigator-usa.com/Article/2019/12/03/Nielsen-Which-sustainability-attributes-matter-most-to-consumers

δείχνουν ότι οι καταναλωτές πληρώνουν εν αγνοία τους τα διπλάσια για το φαγητό τους λόγω τέτοιου κόστους.[51]

Με τον παγκόσμιο πληθυσμό να αναμένεται να εκτιναχθεί από 7 σε 10 δισεκατομμύρια έως το 2056, οι εταιρείες αναζητούν τρόπους να μειώσουν το οικολογικό τους αποτύπωμα.[52]

Εικόνα 38: Η Ασία και η Αφρική αναμένεται να πρωταγωνιστήσουν στην αναμενόμενη αύξηση του παγκόσμιου πληθυσμού μέχρι το 2050



Πηγή: UN Population Review, https://archive-yaleglobal.yale.edu/content/world-population-2020-overview

2.7.5 Φρεσκάδα τροφίμων

Η ζήτηση για φρέσκα τρόφιμα είναι κάτι παραπάνω από μια παροδική μόδα — το 66% των καταναλωτών στις ΗΠΑ αύξησαν τις δαπάνες τους για φρέσκα τρόφιμα σε δύο χρόνια.[53]

Καθώς η αλυσίδα εφοδιασμού τροφίμων προσαρμόζεται στη νέα κανονικότητα, η φρεσκάδα των τροφίμων είναι ακόμη πιο σημαντική. Λόγω της πανδημίας πάνω από το 50% των καταναλωτών δεν αισθάνονται ασφαλείς στα καταστήματα και πλέον ψωνίζουν λιγότερο συχνά, επομένως χρειάζονται φαγητό που διαρκεί ακόμη περισσότερο.[54]

[51] Πηγή: https://sustainablefoodtrust.org/our-work/true-cost-accounting/

[52] Πηγή: https://archive-yaleglobal.yale.edu/content/world-population-2020-overview

[53] Πηγή: https://www.foodnavigator-usa.com/Article/2019/11/13/Deloitte-report-Consumers-fresh-food-spending-on-the-rise

[54] Πηγή: https://www2.deloitte.com/us/en/insights/industry/retail-distribution/future-of-fresh-food-sales/pandemic-consumer-behavior-grocery-shopping.html

Το φαγητό ταξιδεύει πολύ πριν φτάσει στο πιάτο των καταναλωτών. Τα παντοπωλεία είναι κόμβος της παγκοσμιοποίησης. Κατά μέσο όρο, περισσότερες από πέντε χώρες εκπροσωπούνται σε αμερικανικά πιάτα.[55] Αυτό μπορεί να συμβάλει στην αυξημένη αλλοίωση των φρέσκων τροφίμων, λόγω του παρατεταμένου χρόνου μεταφοράς και αποθήκευσης.

Εικόνα 39: Ο όρος «μίλια τροφίμων» περιλαμβάνει την απόσταση που διανύει το φαγητό από την ανάπτυξη στην κατανάλωση, από το έδαφος στο πιάτο. Υπολογίζεται ότι κατά μέσο όρο ένα αμερικανικό γεύμα ταξιδεύει περίπου 1.500 μίλια από την ανάπτυξη στο πιάτο.

Πηγή: https://babylonmicrofarms.com/calculating-the-cost-of-food-miles/

Τα φρέσκα προϊόντα ξοδεύουν πλέον έως και το 50% της διάρκειας ζωής τους κατά τη μεταφορά από το περιβόλι ως το κατάστημα λιανικής.[56] Οι σύνθετες αλυσίδες εφοδιασμού, μαζί με τα κενά μεταξύ παραγωγών, διανομέων και λιανοπωλητών, μειώνουν την ταχύτητα του ταξιδιού και αυξάνουν τις προκλήσεις για τη διατήρηση της φρεσκάδας των τροφίμων.

Καθώς τα τρόφιμα ξεκινούν τη μεταφορά τους μετά τη συγκομιδή, γίνονται τρόπον τινά αόρατα, καθιστώντας δύσκολο να εντοπίσουμε τι συμβαίνει στο 33% της παγκόσμιας προσφοράς των τροφίμων, δηλαδή που χάνεται ή σπαταλάται.[57]

Μια ψηφιακή αλυσίδα εφοδιασμού τροφίμων που τροφοδοτείται από Blockchain επιτρέπει την πλήρη διαφάνεια σε όλο το οικοσύστημα τροφίμων, ούτως ώστε οι έμποροι λιανικής να δύνανται να παρέχουν πιο φρέσκες επιλογές (με αυξημένη διάρκεια ζωής) στους καταναλωτές τους, οδηγώντας σε μειωμένη απώλεια προϊόντων και αυξημένα περιθώρια κέρδους.

[55]Πηγή: https://babylonmicrofarms.com/calculating-the-cost-of-food-miles/

[56]Πηγή: https://www.logmore.com/post/the-challenges-of-fresh-produce-logistics

[57]Πηγή: https://cargodatacorp.com/cost-food-spoilage/

2.7.6 Προβληματικά τρόφιμα

Οι σημερινές ολοένα και πιο περίπλοκες, κατακερματισμένες και παγκόσμιες αλυσίδες εφοδιασμού τροφίμων έχουν οδηγήσει σε απότομη αύξηση της απάτης στα τρόφιμα. Καθοδηγούμενη από την πολυπλοκότητα του σημερινού παγκόσμιου συστήματος τροφίμων, η διατροφική απάτη συνεχίζει να ευδοκιμεί: Είναι μια παγκόσμια επιχείρηση που ξεπερνά τα 50 δισεκατομμύρια δολάρια ετησίως.[58]

Εφόσον υπάρχει κέρδος (και υπάρχει), από το μέλι, το γάλα μέχρι τα ψάρια και το ελαιόλαδο ο κίνδυνος της νοθείας καραδοκεί. Ανεξάρτητα από το επίπεδο των επιπτώσεων στην ασφάλεια ή το πού εμφανίστηκε η ευπάθεια, οι προμηθευτές ευθύνονται σε μεγάλο βαθμό για τον αντίκτυπο, αλλά όλοι στη βιομηχανία τροφίμων υποφέρουν.

Οι σύνθετες αλυσίδες εφοδιασμού δημιουργούν τυφλά σημεία. Πολλές εταιρείες απλώς δεν γνωρίζουν πού και πώς είναι επιρρεπείς σε απάτες τροφίμων. Ωστόσο, με έως και το 10% του συστήματος τροφίμων να επηρεάζεται από απάτη στα τρόφιμα[59], μπορεί να εμφανιστούν αδύναμοι κρίκοι μεταξύ των πρώτων υλών, των συστατικών, των προϊόντων και της συσκευασίας.

Οι ρυθμιστικές αρχές απαιτούν πρακτικές και τεχνολογία αιχμής[60] για να βοηθήσουν τους οργανισμούς να ανταποκριθούν στα πρότυπα και τελικά να δημιουργήσουν ένα πιο διαφανές σύστημα τροφίμων.

Η τεχνολογία Blockchain μπορεί να επιτρέψει την εξοικονόμηση 31 δισεκατομμυρίων δολαρίων (ΗΠΑ) σε απάτες τροφίμων παγκοσμίως έως το 2024 παρακολουθώντας αμετάβλητα τα τρόφιμα σε όλη την αλυσίδα εφοδιασμού και το κόστος συμμόρφωσης μπορεί να μειωθεί κατά 30%.[61]

2.7.7 Κατασπατάληση τροφίμων

Εταιρείες και χώρες στοχεύουν στη μείωση του φαινομένου, οι ΗΠΑ στοχεύουν να μειώσουν στο μισό τη σπατάλη τροφίμων έως το 2030.[62]

Οι ανεπαρκείς υποδομές κρατούν τις εταιρείες στο σκοτάδι. Παρόλο που οι μελέτες υποδεικνύουν ότι η ευρεία υιοθέτηση εργαλείων ψηφιακής αλυσίδας εφοδιασμού θα μπορούσε να μειώσει την απώλεια και τη σπατάλη τροφίμων έως και 120 δισεκατομμύρια USD ετησίως, οι εταιρείες άργησαν να υιοθετήσουν ψηφιακά εργαλεία που θα μπορούσαν να επιτρέψουν την διαφάνεια στην τροφική αλυσίδα και τον εντοπισμό των σημείων όπου συμβαίνει η κατασπατάληση.[63]

[58] Πηγή: https://fsns.com/an-update-on-food-fraud/

[59] Πηγή: https://www.tracegains.com/blog/the-real-cost-of-food-fraud

[60] Πηγή: https://theanalyticalscientist.com/fields-applications/piracy-in-the-pantry

[61] Πηγή: https://www.juniperresearch.com/press/blockchain-to-save-the-food-industry-31-billion

[62] Πηγή: https://www.epa.gov/sustainable-management-food/united-states-2030-food-loss-and-waste-reduction-goal

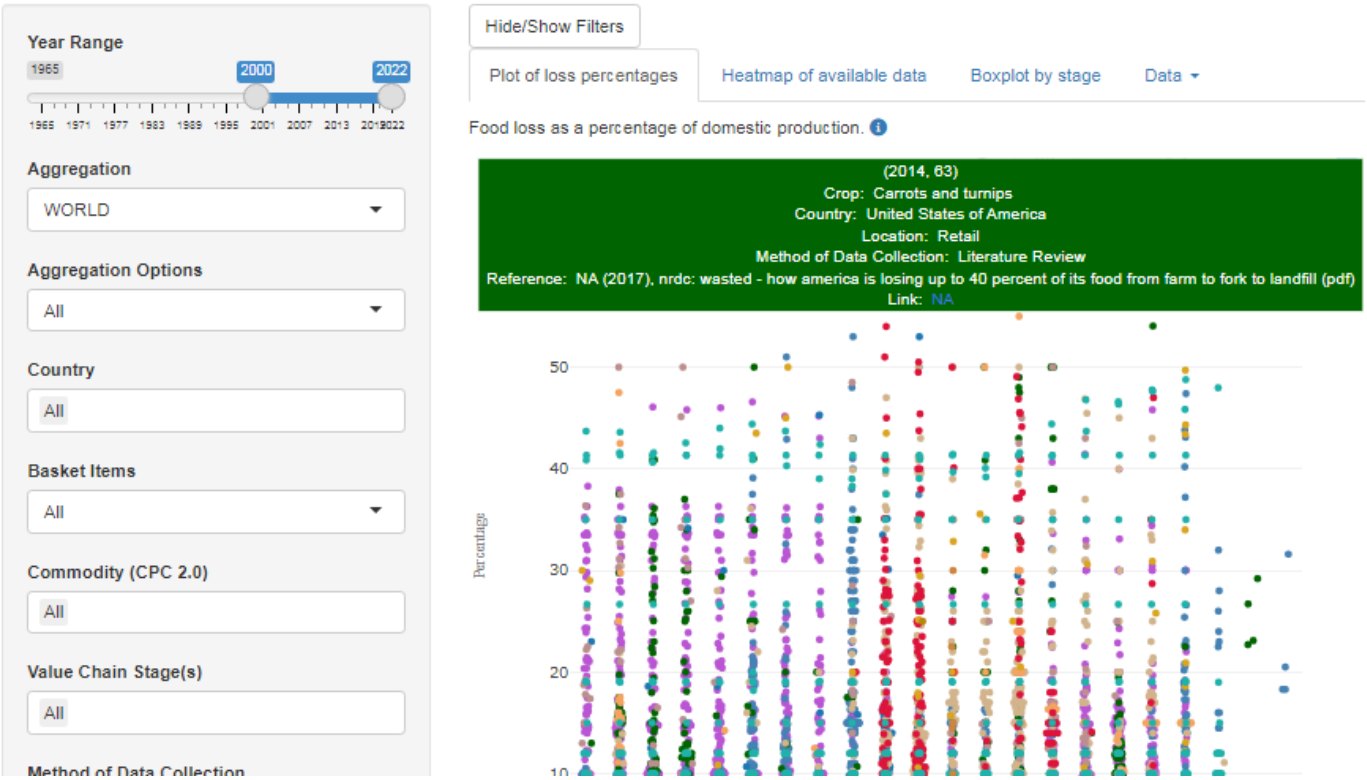
[63] Πηγή: https://www.bcg.com/publications/2018/tackling-1.6-billion-ton-food-loss-and-waste-crisis

Εικόνα 40: Στόχοι βιώσιμης ανάπτυξης

Πηγή: https://www.lifefoster.eu/food-waste-reduction-sustainable-development-goals/

Ο Food and Agriculture Organization των Ηνωμένων Εθνών παρέχει μία πλατφόρμα για ενδελεχή ανάλυση του φαινομένου βάσει επιστημονικών δεδομένων από επιστημονικά περιοδικά, ακαδημαϊκές δημοσιεύσεις και δεδομένα οργανισμών και χωρών.[64]

Εικόνα 41: FAO Food Loss - Waste Database



Πηγή: https://www.fao.org/platform-food-loss-waste/flw-data

[64] Πηγή: https://www.fao.org/platform-food-loss-waste/flw-data

Παρέχει επίσης δύο διαφορετικούς δείκτες, τον Δείκτη Απώλειας Τροφίμων και τον Δείκτη Σπατάλης Τροφίμων, προκειμένου να αξιολογηθεί η επίδοση για τους στόχους Βιώσιμης Ανάπτυξης.[65]

Η παρατήρηση των στοιχείων καθώς η τεχνολογία Blockchain θα εισέρχεται ολοένα και περισσότερο στον τομέα των Μεταφορών, της Αποθήκευσης Προϊόντων και εν γένει της Εφοδιαστικής Αλυσίδας θα έχει ενδιαφέρον καθώς σίγουρα θα περιοριστούν και οι απώλειες και οι σπατάλες.

Εικόνα 42: Δείκτες Απώλειας και Σπατάλης Τροφίμων

Πηγή: https://www.fao.org/sustainable-development-goals/indicators/1231/en/

2.8 Συμπεράσματα 2ου Κεφαλαίου

Η τεχνολογία Blockchain, πέραν της παρεχόμενης Κυβερνοασφάλειας στα ηλεκτρονικά μέσα που τη χρησιμοποιούν, έχει πολλά οφέλη να φέρει στη βιομηχανία των Logistics και την Εφοδιαστική Αλυσίδα όπως αναδείχθηκε σε όλες τις περιπτώσεις που παρουσιάστηκαν. Αυξάνει την αποδοτικότητα σε όλα τα στάδια των διεργασιών των εταιρειών και των οργανισμών, ψηφιοποιώντας κι αυτοματοποιώντας τις διαδικασίες τους, μειώνοντας τη γραφειοκρατία. Προσφέρει διαφάνεια και ιχνηλασιμότητα παρέχοντας μοναδική ασφάλεια σε όλα τα στάδια της εφοδιαστικής αλυσίδας, εφόσον οι πηγές και η αυθεντικότητα των προϊόντων είναι γνωστή, διαπιστευμένη και διαμοιρασμένη.

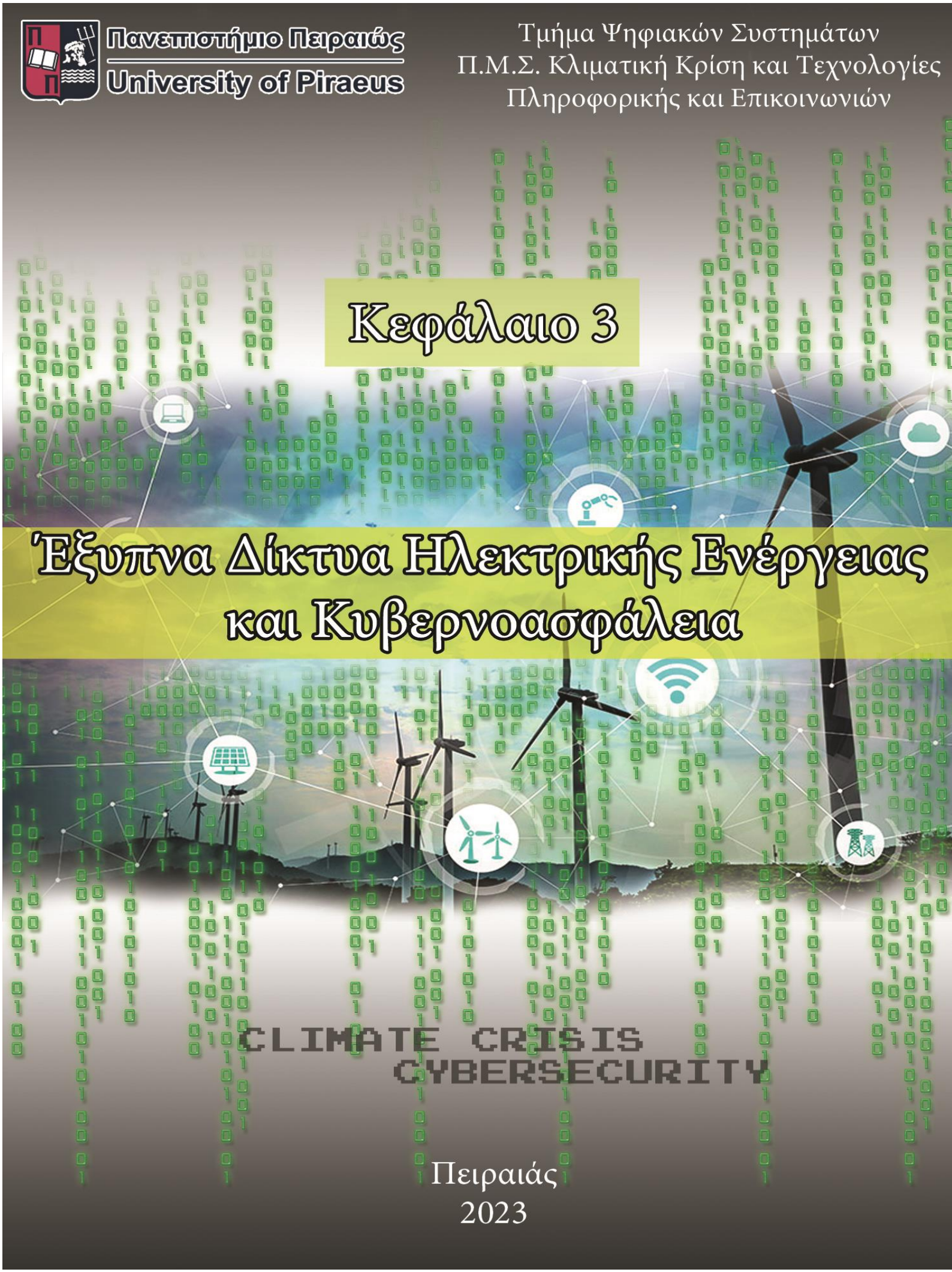
Παρόλα αυτά οι εταιρείες φαίνεται να περιμένουν ακόμα για μία πλήρη υιοθέτηση αυτής της τεχνολογίας, καθώς υπάρχει έλλειψη κατανόησης αυτής και των εφαρμογών της εφόσον τώρα αναπτύσσεται με τη συνεργασία και άλλων τεχνολογιών

[65] Πηγή: https://www.fao.org/sustainable-development-goals/indicators/1231/en/

όπως IoT και 5G-6G. Ρόλο σε αυτό παίζει σίγουρα και το ότι δεν υπάρχει μία μεμονωμένη Blockchain λύση αλλά κάθε εταιρεία ή οργανισμός που υιοθετεί αυτή τη τεχνολογία στον κλάδο τους, την προσαρμόζουν ανάλογα των αναγκών τους.

Βάσει των παραδειγμάτων, των εφαρμογών και των λύσεων που παρουσιάστηκαν, καθίσταται σαφές ότι πρόκειται για ένα πρωτόκολλο ασφαλείας το οποίο αποτελεί την εξέλιξη της αμοιβαίας εμπιστοσύνης και ανάπτυξης και στην εφοδιαστική αλυσίδα αλλά και όπου υλοποιείται, κυρίως λόγω της διαφάνειας και της ιχνηλασιμότητας από τα οποία διέπεται.

Έπειτα από την ανάλυση του πρωτοκόλλου του μέλλοντος Blockchain, στο επόμενο κεφάλαιο αναλύονται οι αρχές της Κυβερνοασφάλειας στον τομέα της Ενέργειας και των Έξυπνων Πόλεων και συγκεκριμένα στα Έξυπνα Δίκτυα Παροχής Ηλεκτρικού Ρεύματος του μέλλοντος.


Πανεπιστήμιο Πειραιώς
University of Piraeus
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Κλιματική Κρίση και Τεχνολογίες Πληροφορικής και Επικοινωνιών
Κεφάλαιο 3
Έξυπνα Δίκτυα Ηλεκτρικής Ενέργειας και Κυβερνοασφάλεια
CLIMATE CRISIS
CYBERSECURITY
Πειραιάς
2023

3.1 Εισαγωγή 3ου Κεφαλαίου

Η τεχνολογία Smart Grid πρόκειται να φέρει επανάσταση στις σύγχρονες βιομηχανίες με ισχυρές λύσεις που εξελίσσουν την αποτελεσματικότητα των παραδοσιακών ηλεκτρικών δικτύων. Το Smart Grid είναι ένα δίκτυο παροχής ηλεκτρικής ενέργειας που χρησιμοποιεί τεχνολογία ψηφιακών επικοινωνιών. Το αυξανόμενο φορτίο και οι απαιτήσεις κατανάλωσης αυξάνουν τις επιπλοκές στα υπάρχοντα δίκτυα. Επί παραδείγματι, η ζήτηση έχει αυξηθεί και τα προβλήματα προέρχονται από διακοπές ρεύματος, υπερφόρτωση και πτώση τάσης. Επιπλέον, το τρέχον ηλεκτρικό δίκτυο αυξάνει τις κρίσιμες εκπομπές άνθρακα καιη ολοένα αυξανόμενη επέκταση του εντείνει την ανάγκη γιατην αντιμετώπιση τωνκυβερνοεπιθέσεων.[66] Οι Ηνωμένες Πολιτείες λαμβάνουν μαζί τους έως και σαράντα τοις εκατό (40%) των εκπομπών διοξειδίου του άνθρακα από τα συστήματα ηλεκτροπαραγωγής σε όλη τη χώρα, γεγονός που βλάπτει το περιβάλλον.

Η ζήτηση για τροφοδοσία ρεύματος έχει αυξηθεί έντονα είτε πρόκειται για οικιακές είτε για εμπορικές περιοχές, λόγω της προόδου στις νέες αναδυόμενες τεχνολογίες που χρησιμοποιούν τα μηχανήματα,και τις συσκευές περισσότερο από πριν. Για αυτούς τους λόγους, η απαίτηση ισχύος έχει αυξηθεί δραματικά. Το παραδοσιακό σύστημα Grid είναι ανεπαρκές για την παροχή των υπηρεσιών σύμφωνα με τα πρότυπα, ενώ το Smart Grid είναι το σύστημα ηλεκτρικής ενέργειας επόμενης γενιάς που θα τεκμηριώσει την ισχύ για τις μεταποιητικές βιομηχανίες.

Με την ενσωμάτωση προηγμένων τεχνολογιών όπως τα εξελιγμένα τηλεπικοινωνιακά συστήματα και η προηγμένη υπολογιστική ισχύς αναμένεται να προσφέρει βελτίωση στην απόδοση, την αξιοπιστία και τη διαθεσιμότητα.[67] Συν τοις άλλοις, το Smart Grid παρέχει υποδομή που είναι ενσωματωμένη με αμφίδρομη επικοινωνία και ροές ηλεκτρικής ενέργειας. Πρόκειται για μια οργανωμένη τεχνολογία όπου η κληρονομιά του είναι οι παραδοσιακές τεχνικές παραγωγής ενέργειας που χρησιμοποιούν φυσικό αέριο, ορυκτά καύσιμα, άνθρακα καθώς και ανανεώσιμες πηγές ενέργειας, όπως ανεμογεννήτριες και ηλιακή ενέργεια.

Παρέχει καλά οργανωμένη διανομή και κατανάλωση ενέργειας σε ένα δίκτυο έξυπνων συσκευών, μηχανών και μετασχηματιστών. Για την επίτευξη αυτών των στόχων χρησιμοποιεί αμφίδρομη επικοινωνία, ενώ το παλαιού τύπου σύστημα πλέγματος χρησιμοποιεί μονόδρομη επικοινωνία. Το Έξυπνο Δίκτυο προσφέρει γρήγορες και βελτιωμένες υπηρεσίες για τους πελάτες, με μειωμένο χρόνο καθυστέρησης απόκρισης όπου η ενεργειακή κρίση μπορεί να επιτευχθεί με αποτελεσματική εφαρμογή.

Ωστόσο, η τεχνολογία Smart Grid συνοδεύεται από τρωτά σημεία και ευπάθειες, με τη μεγαλύτερη δυσκολία να είναι η εξασφάλιση της ασφάλειας των πληροφοριών. Οι λόγοι είναι ότι το σύστημα Smart Grid θα ανταλλάσσει συχνά πληροφορίες, οι οποίες λόγω της ευαισθησίας και πολύτιμης σημασίας τους θα πρέπει να παραμένουν αναλλοίωτες και ακέραιες.

Η Κυβερνοασφάλεια στο Έξυπνο Δίκτυο αποτελεί συνεπώς ύψιστη προτεραιότητα εφόσον πολυάριθμες συσκευές μεμονωμένες είτε εμπορικές, είτε οικιακές θα συνδέονται μέσω μιας σειράς δικτύων για την επικοινωνία και την

[66] Πηγή: Liu J, Xiao Y, Li S, et al. (2012) Cyber security and privacy issues in smart grids. IEEE CommunSurv Tut 14: 981–997.

[67] Πηγή: Dileep G (2020) A survey on smart grid technologies and applications. Renew Energ 146: 2589–2625.

παροχή της ασφάλειας στα δίκτυα με διάφορες τεχνικές.[68] Αυτά τα ζητήματα αποτελούν μία πρόκληση και απαιτούν την παροχή λύσεων και τη λήψη κατάλληλων μέτρων στα πολύπλοκα αυτά προβλήματα ασφάλειας.

3.2 Τι είναι τα Smart Grids;

Τα Έξυπνα Δίκτυα έγιναν γνωστά πριν από μια δεκαετία και είναι απαραίτητα στον ψηφιακό μετασχηματισμό του τομέα της ηλεκτρικής ενέργειας. Η πλειονότητα των υφιστάμενων ηλεκτρικών μας δικτύων είναι παλιάς δεκαετίας και κατασκευάστηκαν όταν οι ανάγκες σε ηλεκτρική ενέργεια ήταν απλές. Οι συνεχώς μεταβαλλόμενες και αυξανόμενες ενεργειακές απαιτήσεις του 21ου αιώνα επιβάλλουν τον εκσυγχρονισμό παρόντα ηλεκτρικά δίκτυα.

Εικόνα 43: Τεχνολογία SmartGrid

Πηγή: https://www.aimspress.com

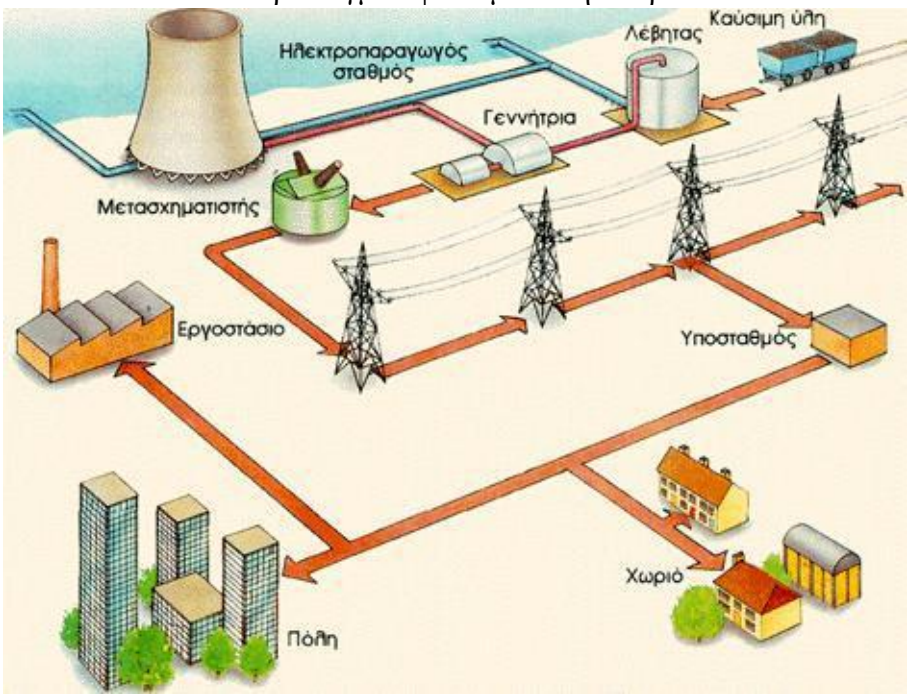
Το Έξυπνο Δίκτυο είναι ένα δίκτυο ηλεκτρικής ενέργειας που διευκολύνει μια αμφίδρομη ροή δεδομένων και ηλεκτρικής ενέργειας χρησιμοποιώντας τεχνολογία ψηφιακών επικοινωνιών, η οποία επιτρέπει τον εντοπισμό, την δυναμική αντίδραση και την προληπτική απόκριση σε αλλαγές στη χρήση και σε διάφορα άλλα ζητήματα. Επιπλέον, τα Έξυπνα Δίκτυα διαθέτουν ικανότητες αυτοθεραπείας σε περίπτωση βλαβών και παρέχουν τη δυνατότητα στους πελάτες ηλεκτρικής ενέργειας να συμμετέχουν ενεργά στο όλο σύστημα.

Η μετάβαση από τα παραδοσιακά ηλεκτρικά δίκτυα στα Έξυπνα Δίκτυα καθοδηγείται από πολλούς παράγοντες, όπως την απορρύθμιση της αγοράς ενέργειας, τις εξελίξεις στη μέτρηση, τις αλλαγές στο επίπεδο παραγωγής ηλεκτρικής ενέργειας, την αποκέντρωση (κατανεμημένη ενέργεια), την έλευση του εμπλεκόμενου «καταναλωτή», την αλλαγή των κανονισμών, την άνοδο της μικροπαραγωγής και των απομονωμένων μικροδικτύων. Τέλος εξαρτάται δυναμικά, όχι μόνο από την εμπλοκή των ανανεώσιμων πηγών ενέργειας στο ενεργειακό μίγμα, αλλά κι από ακόμα

[68] Πηγή: Maglaras LA, Kim KH, Janicke H, et al. (2018) Cyber security of critical infrastructures. Ict Express 4: 42–45.

περισσότερες πηγές ενέργειας και νέα σημεία και σκοπούς για τους οποίους απαιτείται ηλεκτρική ενέργεια, όπως τα σημεία φόρτισης των ηλεκτρικών οχημάτων.

Εικόνα 44: Παράδειγμα υφιστάμενου ηλεκτρικού δικτύου



Πηγή: Διπλωματική εργασία, 'Έξυπνα Δίκτυα Ηλεκτρικής Ενέργειας (SmartGrids) και Σύγχρονες Τεχνολογίες Επικοινωνίας', Νικόλαος Σουλτάνος, 2018

Ένα ηλεκτρικό δίκτυο είναι ένα δίκτυο που παρέχει ηλεκτρική ενέργεια από τους παραγωγούς και τους χώρους όπου παράγεται και μετασχηματίζεται, δηλαδή τους σταθμούς και τους υποσταθμούς ηλεκτροπαραγωγής, ως τους τελικούς προορισμούς όπου «καταναλώνεται» η ηλεκτρική ενέργεια δηλαδή στα νοικοκυριά, στις επιχειρήσεις, στις διάφορες εγκαταστάσεις και γενικότερα σε άλλες καταναλωτικές ενέργειες.

Στην πράξη είναι ένα δίκτυο υψηλής διασύνδεσης με πολλά στοιχεία όπως υποσταθμούς, γραμμές μεταφοράς και καλωδιώσεις, γραμμές διανομής, μετασχηματιστές και άλλα.

Ο στόχος της μετάβασης του τρέχοντος ενεργειακού δικτύου σε ένα Έξυπνο Δίκτυο είναι να προσφέρει αξιόπιστη και κορυφαία ηλεκτρική ενέργεια στις ψηφιακές κοινωνίες με φιλικό προς το περιβάλλον και βιώσιμο τρόπο. Αυτός ο στόχος θα επιτευχθεί με την εφαρμογή ενός μείγματος καθιερωμένων και καινοτόμων τεχνολογιών για τη βελτίωση της ενεργειακής απόδοσης, την ενσωμάτωση ανανεώσιμων πηγών ενέργειας, τη διευκόλυνση της ανταπόκρισης στη ζήτηση, τη δυνατότητα παρακολούθησης και ελέγχου ευρείας περιοχής και την προώθηση των δυνατοτήτων αυτοθεραπείας, του συστήματος μετάδοσης ηλεκτρικής ενέργειας συνεχούς ρεύματος υψηλής τάσης (HVDC), του εύκαμπτου συστήματος μεταφοράς εναλλασσόμενου ρεύματος, κ.λπ.

3.2.1 Ορισμοί των Έξυπνων Δικτύων

Ο όρος «Έξυπνο Δίκτυο» δεν είναι ευρέως αποδεκτός και μπορεί να θεωρηθεί ως μια ευρύτερη έννοια που αφορά το μελλοντικό σύστημα ηλεκτρικής ενέργειας.

Διαφορετικές χώρες, περιφέρειες και παράγοντες έχουν τις δικές τους ερμηνείες και κίνητρα για την υιοθέτηση αυτής της έννοιας. Παρακάτω ακολουθούν διαφορετικοί ορισμοί από διαφορετικούς αρμόδιους τομείς: [69]

• Η Ευρωπαϊκή Πλατφόρμα Τεχνολογίας, ορίζει το Έξυπνο Δίκτυο ως «ένα ηλεκτρικό δίκτυο που έχει τη δυνατότητα να ενσωματώνει έξυπνα τις ενέργειες όλων των χρηστών που συνδέονται με αυτό, συμπεριλαμβανομένων των παραγωγών, των καταναλωτών και εκείνων που εκπληρώνουν και τους δύο ρόλους. Αυτή η ενοποίηση στοχεύει στη διευκόλυνση της αποτελεσματικής, βιώσιμης και ασφαλούς παροχής ηλεκτρικής ενέργειας».

• Το Electric Power Research Institute (ERPI), παρουσιάζει το Έξυπνο Δίκτυο ως «μία εξαιρετικά προηγμένη υποδομή παροχής ηλεκτρικής ενέργειας, εξοπλισμένη με τεχνολογίες αιχμής επικοινωνιών, υπολογιστών και ηλεκτρονικών, με στόχο την κάλυψη των μελλοντικών απαιτήσεων ηλεκτρικής ενέργειας της κοινωνίας».

• Σύμφωνα με το Γραφείο Μεταφοράς και Διανομής Ενέργειας των ΗΠΑ (DoE) ως Έξυπνο Δίκτυο ορίζεται «η λύση που στοχεύει να εξασφαλίσει την αξιοπιστία, την ασφάλεια και την αποτελεσματικότητα του ηλεκτρικού συστήματος διευκολύνοντας την ανταλλαγή πληροφοριών, την κατανεμημένη παραγωγή και την αποθήκευση ενέργειας».

• Η Ευρωπαϊκή Επιτροπή περιγράφει το Έξυπνο Δίκτυο ως «ένα εξαιρετικά προηγμένο ηλεκτρικό δίκτυο, το οποίο περιλαμβάνει χαρακτηριστικά όπως αμφίδρομη επικοινωνία μεταξύ παραγωγών και καταναλωτών και έξυπνα συστήματα για τη μέτρηση και την παρακολούθηση της απόδοσής του».

• Τέλος, η Ομάδα Εργασίας της Ευρωπαϊκής Επιτροπής για το Έξυπνο Δίκτυο (European Commission Task Force for Smart Grid) ορίζει το Έξυπνο Δίκτυο ως «ένα ηλεκτρικό δίκτυο που ενσωματώνει αποτελεσματικά τη συμπεριφορά και τις ενέργειες όλων των συνδεδεμένων παραγόντων του, όπως οι παραγωγοί, οι καταναλωτές και οι παραγωγοί ενέργειας, για να εξασφαλίσει ένα οικονομικά αποδοτικό, βιώσιμο ενεργειακό σύστημα με ελάχιστες απώλειες και υψηλής ποιότητας εξυπηρέτηση σε ένα ασφαλές και αξιόπιστο δίκτυο».

Επομένως, δύναται να συναχθεί το συμπέρασμα ότι τα Έξυπνα Δίκτυα ενσωματώνουν τεχνολογίες που βελτιστοποιούν τη διαχείριση των πόρων, όπως τους έξυπνους μετρητές ενέργειας, καθώς και την ακριβή παρακολούθηση όλων των συνδεδεμένων στοιχείων. Ουσιαστικά, δύναται να θεωρηθεί ως η αναβάθμιση του τρέχοντος δικτύου ηλεκτρικής ενέργειας σε ένα δίκτυο που χρησιμοποιεί εφαρμογές τεχνολογιών πληροφορικής και επικοινωνιών.

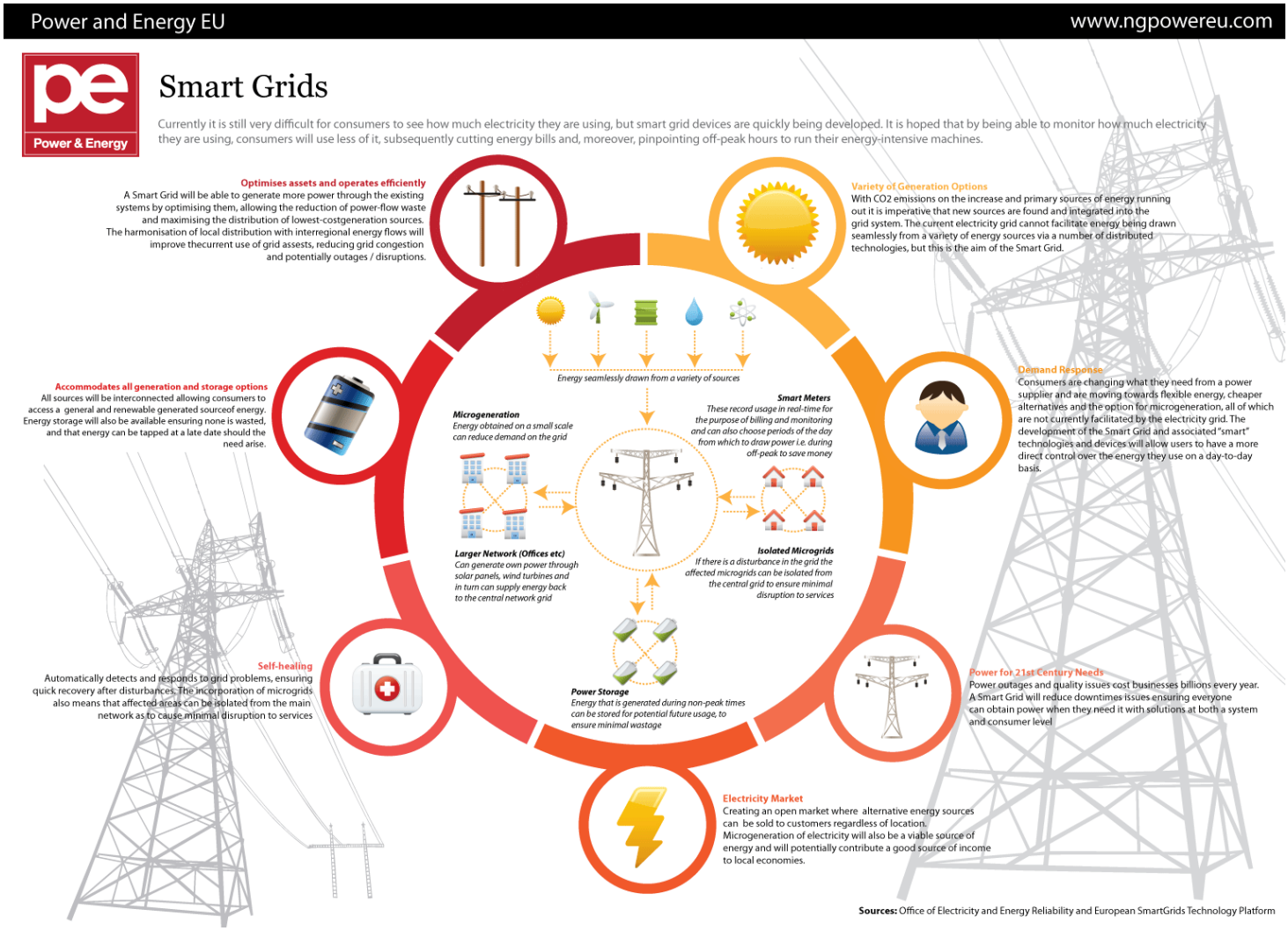
3.3 Το Έξυπνο Δίκτυο σε σύγκριση με τα παραδοσιακά δίκτυα ηλεκτρικής ενέργειας - Η ουσία και οι διαφορές

Τα παραδοσιακά δίκτυα ηλεκτρικής ενέργειας δεν είχαν σχεδόν καθόλου δυνατότητες αποθήκευσης, βασίζονται στη ζήτηση και έχουν ιεραρχική δομή. Σε ένα ηλεκτρικό δίκτυο η τάση μειώνεται σταδιακά, έτσι ώστε η ηλεκτρική ενέργεια να μπορεί να χρησιμοποιηθεί από αυτούς τους διαφορετικούς καταναλωτές: από τα επίπεδα τάσης μετάδοσης έως τα επίπεδα τάσης διανομής και τα επίπεδα τάσης

[69] Πηγή: ΕΥΦΥΗ ΔΙΚΤΥΑ Διπλωματική Εργασία Σιρανίδου Ε. Μιλένα, https://core.ac.uk/download/pdf/323472895.pdf

εξυπηρέτησης (στην πραγματικότητα είναι και ανεβοκατέβασμα και επομένως λίγο πιο περίπλοκο).

Εικόνα 45: Έξυπνα δίκτυα που εξηγούνται από την Power and Energy EU με πολλαπλές πηγές ενέργειας, απομονωμένα μικροδίκτυαμικροπαραγωγής και αποθήκευση ενέργειας. Στο κέντρο φαίνονται τα διάφορα οφέλη αναλυτικά.



Πηγή: https://www.flickr.com/photos/gdsdigital/4035052550

Συνήθως, γίνεται διάκριση μεταξύ μετάδοσης (δίκτυο μετάδοσης: υψηλή και εξαιρετικά υψηλή τάση) και διανομής (δίκτυο διανομής: χαμηλότερη τάση), όπου στην παραπάνω εικόνα (Εικόνα 45), εμφανίζονται διαφορετικά συστήματα καλωδίωσης. Ο σκοπός ενός ηλεκτρικού δικτύου είναι να διασφαλίζει ότι η ηλεκτρική ενέργεια παρέχεται πάντα, όταν και όπου χρειάζεται, χωρίς διακοπές, και εδώ βρίσκονται πολλές προκλήσεις στις οποίες ένα Έξυπνο Δίκτυο μπορεί ήδη να προσφέρει λύσεις.

Δεδομένης της πολυπλοκότητας και των πολλαπλών προκλήσεων που μπορεί να προκύψουν, όπως οι συνέπειες των δυσμενών καιρικών συνθηκών, οι ζημιές από την άγρια ζωή, η ανθρώπινη δολιοφθορά και άλλοι εξωτερικοί παράγοντες και εσωτερικοί παράγοντες (ζητήματα με αστοχία εξοπλισμού και κρίσιμα στοιχεία), η διαχείριση ενός δικτύου είναι πολύ περίπλοκη και υπάρχουν και οι ειδικοί που πρέπει

επίσης να εξετάσουν τις επιλογές σχετικά με τους ενεργειακούς κανονισμούς και τις πρωτοβουλίες αειφορίας από τις κυβερνήσεις.

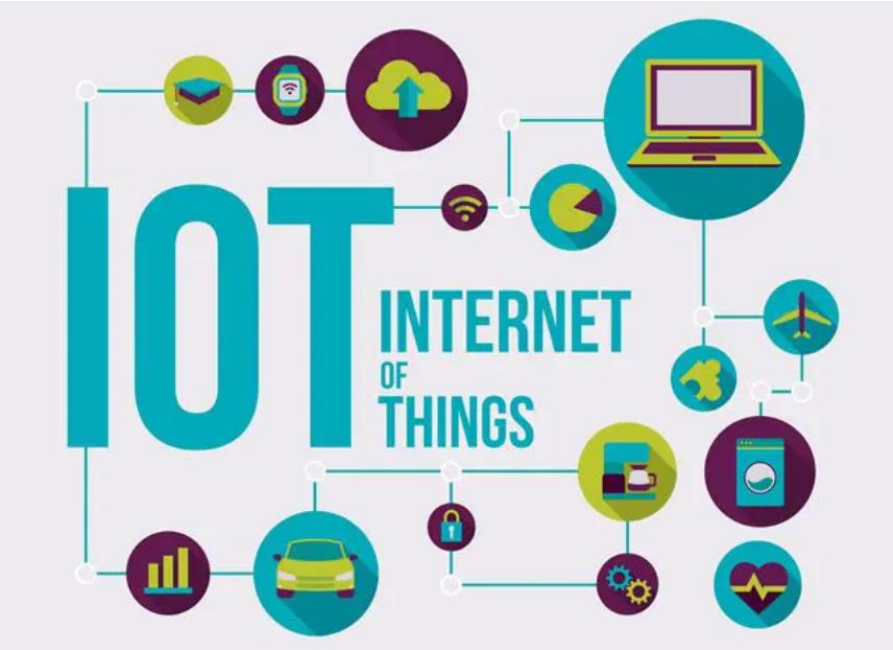
Στα Έξυπνα Δίκτυα, οι δυνατότητες αυτοΐασης επιτρέπουν την αυτόματη ανίχνευση και απόκριση σε προβλήματα δικτύου και τη διασφάλιση γρήγορης ανάκτησης μετά από διαταραχές.

Η αμφίδρομη ροή ηλεκτρικής ενέργειας και δεδομένων που είναι το βασικό χαρακτηριστικό ενός Έξυπνου Δικτύου επιτρέπει την τροφοδοσία πληροφοριών και δεδομένων στους διάφορους ενδιαφερόμενους στην αγορά ηλεκτρικής ενέργειας, τα οποία μπορούν να αναλυθούν για τη βελτιστοποίηση του δικτύου, την πρόβλεψη πιθανών ζητημάτων, την γρηγορότερη αντίδραση όταν προκύπτουν προκλήσεις και να δημιουργήσουν νέες δυνατότητες – και υπηρεσίες – καθώς το τοπίο της ενέργειας αλλάζει.

Η αγορά ηλεκτρικής ενέργειας, η κατανάλωση ηλεκτρικής ενέργειας, οι κανονισμοί, οι απαιτήσεις διαφόρων ενδιαφερομένων και η ίδια η παραγωγή ηλεκτρικής ενέργειας αλλάζουν. Έτσι, πρωτοβουλίες Έξυπνου Δικτύου υπάρχουν σε όλο τον κόσμο, αν και μερικές φορές με διαφορετικές προσεγγίσεις και στόχους.

Ενώ το Έξυπνο Δίκτυο εξακολουθεί να αναφέρεται στην αμφίδρομη μετάδοση δεδομένων και ηλεκτρικής ενέργειας (με τους προμηθευτές και τους οργανισμούς που παράγουν επίσης ηλεκτρική ενέργεια), η έννοια και η εμβέλεια του όρου έχει διευρυνθεί λόγω των πολλών δυνατοτήτων που παρέχει αυτή η σημαντική αλλαγή και οι ολοένα και περισσότερες τεχνολογίες που χρησιμοποιούνται σε πλαίσιο ανάπτυξης Έξυπνων Δικτύων.

Εικόνα 46: Internet of Things



Πηγή: https://www.i-scoop.eu/internet-of-things

Σημαντικό ρόλο στην τεχνολογία των Έξυπνων Δικτύων δύναται να κατέχουν όλων των ειδών οι νέες τεχνολογίες όπως το Διαδίκτυο των Πραγμάτων (IoT) εφόσον στην υλοποίηση τους εμπλέκεται η διασύνδεση αισθητήρων, τα μεγάλα δεδομένα, οι προηγμένες αναλύσεις με Τεχνητή Νοημοσύνη και μηχανική μάθηση και άφθονα πρότυπα επικοινωνίας που χρησιμοποιούνται για την αποστολή δεδομένων από το ένα σημείο στο άλλο (π.χ. από έξυπνους μετρητές σε εταιρείες κοινής ωφέλειας).

Επιπλέον περισσότερες τεχνολογίες όπως τα λεγόμενα ψηφιακά δίδυμα, εμφανίζονται στον ψηφιακό μετασχηματισμό των υπηρεσιών κοινής ωφέλειας και στη βιομηχανία.

Η ολοένα αυξανόμενη υπολογιστική εξέλιξη μέσω των Edge Computing και των Edge Analytics βελτιώνει την απόδοση και την επεξεργασία των λογισμικών, των υπολογιστικών πόρων και όλων των συνεργαζόμενων βοηθητικών προγραμμάτων και τεχνολογιών συνολικά.

3.3.1 Τα πλεονεκτήματα του Έξυπνου Δικτύου

Τα Έξυπνα Δίκτυα προσφέρουν ένα ευρύ φάσμα βελτιώσεων και πλεονεκτημάτων σε διάφορους τομείς, συμπεριλαμβανομένης της αξιοπιστίας και ασφάλειας του δικτύου, των οικονομικών οφελών, των μειωμένων περιβαλλοντικών επιπτώσεων και της ενδυνάμωσης του ρόλου των καταναλωτών. Παρακάτω παρουσιάζονται τα χαρακτηριστικά ενός Έξυπνου Δικτύου καθώς και το πώς αναμένεται να βελτιώσουν το τρέχον σύστημα δικτύου.[70]

1. Αξιοπιστία: Το Έξυπνο Δίκτυο, που λειτουργεί σαν ζωντανός οργανισμός, έχει τη δυνατότητα να εντοπίζει προβλήματα και να ρυθμίζει αποτελεσματικά τη διανομή της ενέργειας ή να απομονώνει μια συγκεκριμένη περιοχή που δεν λειτουργεί εντός των επιθυμητών παραμέτρων, προκειμένου να ελαχιστοποιούνται οι απώλειες. Η ιδιότητα αυτή, η οποία συνήθως αναφέρεται ως αυτοΐαση (self-healing) ενισχύει την ικανότητα του δικτύου να αντέχει σε εξωτερικές διαταραχές.
2. Αποδοτικότητα: Το Δίκτυο διαχειρίζεται τους πόρους που χρειάζεται για να καλύψει τις αυξημένες ενεργειακές απαιτήσεις χωρίς να απαιτεί πρόσθετη υποδομή. Επιπλέον παράδειγμα είναι ο αυτοέλεγχος των τεχνικών μέσων (εξοπλισμός) για την έγκαιρη αντικατάστασή τους, ο οποίος ελαχιστοποιεί το κόστος που σχετίζεται με την αγορά του εξοπλισμού και το χρονοδιάγραμμα της ενδεχόμενης αντικατάστασής του.
3. Ευελιξία: Το Έξυπνο Δίκτυο διευκολύνει τη σύνδεση τόσο πηγών ενέργειας (όπως Ανανεώσιμες Πηγές Ενέργειας) πολλών και διαφόρων μεγεθών και τεχνολογιών, όσο και κεντρικών σταθμών παραγωγής ενέργειας, πηγών αποθήκευσης ενέργειας, μικρών συστημάτων συμπαραγωγής και άλλων πηγών κατανεμημένης παραγωγής.
4. Απελευθέρωση της αγοράς: Με νέες ευκαιρίες, αγορές και υπηρεσίες, οι καταναλωτές δύνανται να επιλέξουν τις πιο ευνοϊκές συνθήκες για αυτούς, ενώ οι μικρές επιχειρήσεις μπορούν να ανταγωνίζονται μέσω καινοτόμων προσεγγίσεων.
5. Ποιότητα ενέργειας: η απαιτούμενη ποιότητα ενέργειας παρέχεται για την εξυπηρέτηση πελατών με διαφορετικές ανάγκες. Η διασφάλιση ποιότητας θα συνεπάγεται αντίστοιχο κόστος, ενώ με εξελιγμένο εξοπλισμό θα πραγματοποιούνται σύγχρονες μέθοδοι παρακολούθησης οι οποίες θα επιτρέπουν την έγκαιρη διάγνωση τυχόντων προβλημάτων και την εξάλειψη των αιτιών υποβάθμισης της ποιότητας ισχύος.
6. Ενδυνάμωση του καταναλωτή: Κύριο στοιχείο του Έξυπνου Δικτύου είναι η εξοικονόμηση και η ανατροφοδότηση πόρων που παρέχονται στον καταναλωτή. Οι διαρκώς και ανά πάσα στιγμή ενημερωμένοι καταναλωτές σχετικά με τη χρήση ενέργειας δύνανται να προσαρμόζουν την κατανάλωσή

[70] Πηγή: Miller J , The Smart Grid – Benefits and Challenges ,EEI Annual Convention – Toronto, Modern Grid Strategy Team June 16, 2008

τους βάσει των οικονομικών και περιβαλλοντικών οφελών ώστε να εξισορροπείται η ζήτηση και η προσφορά ενέργειας. Επί παραδείγματι, οι πάροχοι ορίζοντας ώρες αιχμής ζήτησης θα επιβραβεύουν την αποχή των καταναλωτών από δραστηριότητες έντασης ενέργειας στο σύστημα. Η ενσωμάτωση έξυπνων μετρητών, έξυπνων συσκευών και άλλων τεχνολογιών στο δίκτυο θα πρέπει να επιτρέψει όχι μόνο τις παραπάνω δυνατότητες αλλά και την παροχή κοινωνικής ευαισθητοποίησης για ευπαθείς ομάδες και κρατικών κινήτρων.

7. Φιλικό προς το περιβάλλον: Η μεγάλης κλίμακας ενσωμάτωση των Ανανεώσιμων Πηγών Ενέργειας θα μετατρέψει αποτελεσματικά το Έξυπνο Δίκτυο σε ένα κυρίως «πράσινο», συμβάλλοντας με αυτόν τον τρόπο στην προστασία του περιβάλλοντος.

Εν τέλει, οι απαιτήσεις για την επόμενη γενιά δικτύων παροχής ηλεκτρικού ρεύματος είναι υψηλές καθώς αυτά, τώρα περισσότερο από ποτέ με την ταχεία ανάπτυξη της τεχνητής νοημοσύνης, αναμένονται να είναι περισσότερο ευφυή, αλλά και ανθεκτικά τόσο σε διάφορα είδη κακόβουλων επιθέσεων όσο και σε φυσικές καταστροφές. Συν τοις άλλοις, με την αυτορύθμισή τους, εξασφαλίζεται η ικανοποίηση των προσωπικών αναγκών των καταναλωτών.

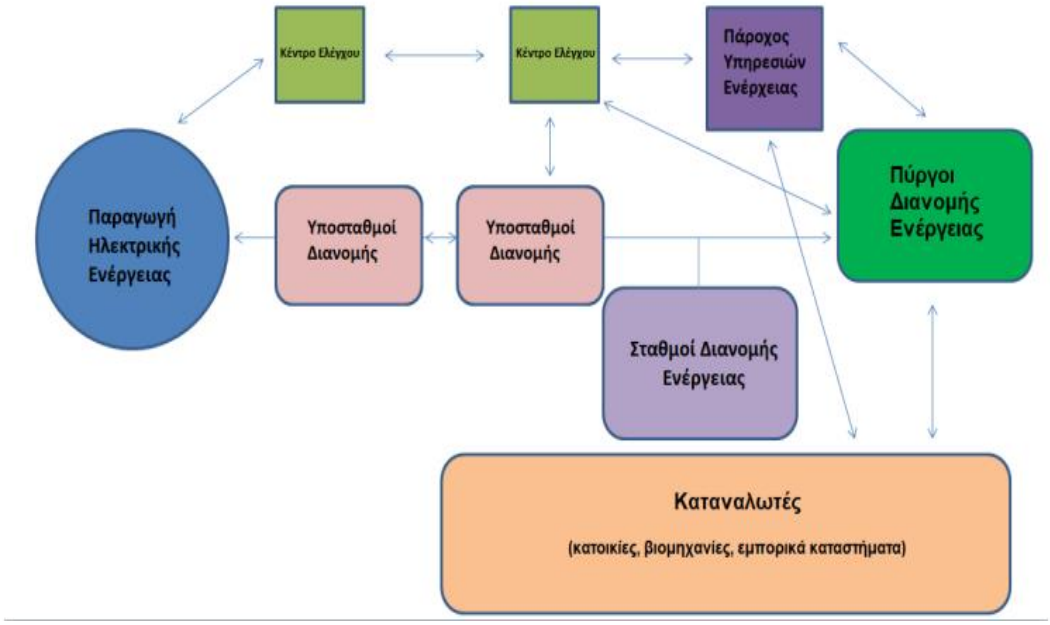
3.3.2 Η δομή των Έξυπνων Δικτύων

Παρόμοια με οποιοδήποτε παραδοσιακό δίκτυο, το Έξυπνο Δίκτυο περιλαμβάνει διάφορες διασυνδεδεμένες λειτουργικές μονάδες. Από γεννήτριες ηλεκτρικής ενέργειας, υποσταθμούς ηλεκτρικής ενέργειας, γραμμές μεταφοράς και διανομής, ελεγκτές, έξυπνους μετρητές έως κόμβους συλλογής και κέντρα ελέγχου διανομής και μεταφοράς. Στο σύνολο της βιβλιογραφίας, τα προαναφερθέντα στοιχεία σχηματίζουν τα εξής διαφορετικά συστήματα:[71]

- Έξυπνο σύστημα υποδομής: Ευθύνεται για την ενέργεια, την επικοινωνία και τις πληροφορίες στα οποία βασίζεται το Ευφυές Δίκτυο, και υλοποιεί:
  1) την έξυπνη παραγωγή, μεταφορά και κατανάλωση ενέργειας,
  2) την έξυπνη μέτρηση, παρακολούθηση και διαχείριση ενέργειας και
  3) τις ανεπτυγμένες τεχνολογίες επικοινωνίας.
- Έξυπνο σύστημα Διαχείρισης: Διαχειρίζεται και ελέγχει την ενέργεια, ώστε να μεγιστοποιείται η ενεργειακή απόδοση, να βελτιώνονται τα χαρακτηριστικά, να μειώνεται το κόστος και να ελέγχονται οι εκπεμπόμενοι ρύποι.
- Έξυπνο σύστημα Προστασίας: Ευθύνεται για την ομαλή λειτουργία και ασφάλεια του Έξυπνου Δικτύου.

[71] Πηγή: C. Li et al., "Grid architecture for future distribution system — A cyber-physical system perspective," IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 5235-5239

Εικόνα 47: Διασύνδεση στοιχείων Έξυπνου Δικτύου



3.4 Τα οφέλη του Έξυπνου Δικτύου σε αριθμούς

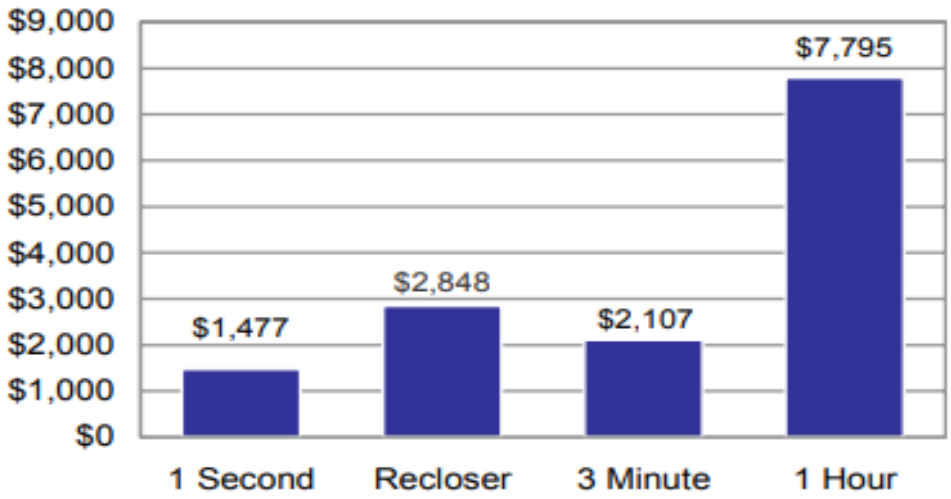
Τα οφέλη του Έξυπνου Δικτύου, όπως αναφέρθηκε και παραπάνω, περιλαμβάνουν τη βελτιωμένη απόδοση και αξιοπιστία της παροχής ηλεκτρικής ενέργειας, την ενσωμάτωση περισσότερων ανανεώσιμων πηγών ενέργειας στο υπάρχον δίκτυο, την υποστήριξη της ανάπτυξης ηλεκτρικών οχημάτων σε κλίμακα τις νέες λύσεις για τους πελάτες για βελτιστοποίηση της κατανάλωσης ηλεκτρικής ενέργειας και μείωση των εκπομπών άνθρακα. Το Ευφυές Δίκτυο δεν αφορά μόνο τη βελτίωση της υπάρχουσας υποδομής αλλά και την αξιοποίηση του πλήρους δυναμικού του δικτύου. Υπόσχεται ένα σύστημα χαμηλών εκπομπών άνθρακα, ένα «πράσινο», αποδοτικό και καθαρό ενεργειακό σύστημα. Συνεπώς, όσο πιο γρήγορα αναπτυχθούν τόσο πιο γρήγορα θα μετριαστεί και το φαινόμενο της κλιματικής κρίσης.

Καθώς οι οικονομίες έχουν αρχίσει να εξαρτώνται από την άντληση δεδομένων και τη χρήση των υπολογιστών στις περισσότερες παραγωγικές διαδικασίες, η ανάγκη για ένα σταθερό και αξιόπιστο δίκτυο ηλεκτροδότησης θα έπρεπε να αποτελεί προτεραιότητα για τις κυβερνήσεις των κρατών. Η αυξανόμενη εξάρτηση της κοινωνίας από τα ψηφιακά κυκλώματα έχει ως αποτέλεσμα ακόμη και σύντομες διαταραχές στο δίκτυο να είναι ιδιαίτερα δαπανηρές. Πέρα από τις διακοπές, που αποτελούν απώλεια ρεύματος και μπορεί να διαρκέσουν από κλάσματα δευτερολέπτων έως και αρκετές ώρες, πρόβλημα στο δίκτυο προκαλεί η χαμηλής ποιότητας παροχή και παρατηρούνται φαινόμενα όπως πτώση τάσης, υπερτάσεις και μεταβατικές καταστάσεις.

Στις Ηνωμένες Πολιτείες Αμερικής, λαμβάνοντας δεδομένα από 985 επιχειρήσεις που δραστηριοποιούνται στους κλάδους της ψηφιακής οικονομίας, των κατασκευών και της κλωστοϋφαντουργίας, το κόστος από τη διακοπή ρεύματος (που προκαλεί την απώλεια της παραγωγής ή των πωλήσεων, βλάβες στα μηχανήματα,

απώλειες πρώτων υλών, κλπ) εκτιμάται κατά μέσο όρο από 1.477 δολάρια για διακοπή 1 δευτερολέπτου έως 7.795 δολάρια εάν αυτή διαρκέσει 1 ώρα. [72]

Εικόνα 48: Το κόστος των αποσυνδέσεων στις ΗΠΑ



Πηγή: https://www.epri.com/research/products

Τα Έξυπνα Δίκτυα παρέχουν μεγαλύτερη αξιοπιστία στο δίκτυο καθώς με τη χρήση τους μειώνεται η διάρκεια και η συχνότητα των blackout και των διακοπών λειτουργίας του ηλεκτρικού δικτύου. Τα κόστη που προκύπτουν για την επαναλειτουργία του δικτύου μειώνονται παρέχοντας ποιοτικότερες υπηρεσίες στον τελικό καταναλωτή. Για το 2001, το Ινστιτούτο Ερευνών Ηλεκτρικής Ενέργειας (ERPI) των Ηνωμένων Πολιτειών Αμερικής, το κόστος από διακοπές ρεύματος και άλλες διαταραχές υπολογίστηκε στα 119 δισεκατομμύρια δολάρια. Συν τοις άλλοις, οι τελικοί καταναλωτές επωφελούνται από ένα σταθερό ηλεκτρικό δίκτυο έχοντας μειωμένους λογαριασμούς.

3.5 Ανάγκη για τις νέες τεχνολογίες

Η ηλεκτρική ενέργεια παίζει ζωτικό ρόλο στην καθημερινή μας ζωή και χρησιμεύει ως βάση για τις καθημερινές μας δραστηριότητες. Το ηλεκτρικό δίκτυο αποτελείται από τρία κύρια υποσυστήματα: τις μονάδες παραγωγής ενέργειας, τα δίκτυα μεταφοράς και διανομής και τους διάφορους τελικούς χρήστες, όπως τα σπίτια, τα καταστήματα και τις βιομηχανίες. Η διατήρηση μιας ισορροπίας μεταξύ προσφοράς και ζήτησης ηλεκτρικής ενέργειας είναι ζωτικής σημασίας σε ένα σύστημα ηλεκτρικού δικτύου, καθώς η αποθήκευση ηλεκτρικής ενέργειας σε μεγάλη κλίμακα δεν είναι εφικτή. Ιστορικά, αυτή η ισορροπία διατηρήθηκε από αρχές διαχείρισης ενέργειας που επέβλεπαν τον έλεγχο της παραγωγής και της μεταφοράς ενέργειας.

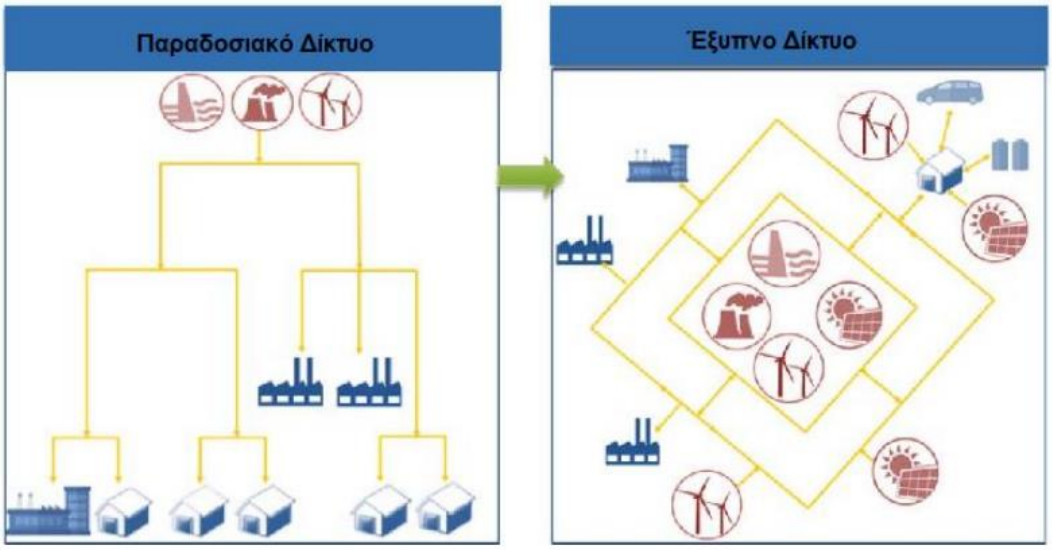
Οι μεταβαλλόμενες ανάγκες της σημερινής βιομηχανικής δραστηριότητας έχουν καταστήσει τα παραδοσιακά ενεργειακά δίκτυα ακατάλληλα για την αντιμετώπιση των σημαντικών διαφορών στις προδιαγραφές σε σύγκριση με όταν

[72] Πηγή: (David Lineweber, The Cost of Power Disturbances to, 2001)

κατασκευάζονταν πριν από δεκαετίες. Συγκεκριμένα, η απελευθέρωση της αγοράς ενέργειας έχει εισαγάγει σενάρια ροής ενέργειας και αβεβαιότητες που το σύστημα δεν σχεδιάστηκε αρχικά να χειρίζεται. Επιπρόσθετα, η αυξανόμενη παραγωγή «πράσινης» ενέργειας έχει αποκεντρώσει την παραγωγή ενέργειας, με αποτέλεσμα να υπάρχουν αβεβαιότητες εφοδιασμού. Επιπλέον, ο σύγχρονος τρόπος ζωής μας βασίζεται σε μεγάλο βαθμό στο αγαθό αυτό και απαιτεί παροχή ηλεκτρικού ρεύματος υψηλής ποιότητας και άμεσα διαθέσιμης. Είναι πλέον πιο σημαντικό από ποτέ η παραγωγή και η διαχείριση ενέργειας να πραγματοποιούνται με τρόπο φιλικό προς το περιβάλλον, κάτι που μπορεί να επιτευχθεί μέσω των ανανεώσιμων πηγών ενέργειας και της βελτιστοποίησης της ενεργειακής απόδοσης με ταυτόχρονη μείωση της ζήτησης.

Η ολοένα και πιο διαδεδομένη πεποίθηση στον κλάδο είναι ότι η τεχνολογία Smart Grid παρέχει τη λύση στις προαναφερθείσες προκλήσεις. Αυτό φαίνεται από τις σημαντικές επενδύσεις που πραγματοποιήθηκαν από τις Ηνωμένες Πολιτείες της Αμερικής, την Ευρωπαϊκή Ένωση και την Κίνα στην έρευνα και ανάπτυξη τεχνολογιών Smart Grid. Ο στόχος της μετάβασης σε ένα Έξυπνο Δίκτυο είναι η παραγωγή αξιόπιστης, κορυφαίας ποιότητας ηλεκτρική ενέργεια στις ψηφιακές κοινωνίες, ενώ ταυτόχρονα οφείλει να είναι περιβαλλοντικά καθαρή και βιώσιμη. Για την επίτευξη αυτού του στόχου, είναι απαραίτητο να συγχωνευθεί η υπάρχουσα γνώση με την εφαρμογή νέων τεχνολογιών για τη βελτίωση της ενεργειακής απόδοσης, την ενσωμάτωση των ανανεώσιμων πηγών ενέργειας, τη διευκόλυνση της ανταπόκρισης στη ζήτηση, την προώθηση της αυτοθεραπείας κ.λπ.

Εικόνα 49: Μετάβαση από το παρόν Δίκτυο στο Έξυπνο Δίκτυο



Πηγή: Grid architecture for future distribution system. A cyber-physical system perspective. ieeexplore.ieee.org

Το Έξυπνο Δίκτυο επιδεικνύει ένα εντυπωσιακό επίπεδο ευφυΐας αυτόματης λήψης αποφάσεων. Αυτή η ιδέα περιλαμβάνει διασυνδεδεμένα συστήματα ηλεκτρικής ενέργειας, τόσο συγκεντρωμένης μαζικής παραγωγής όσο και κατανεμημένης παραγωγής. Εκτείνεται από τα συστήματα μετάδοσης υψηλής τάσης έως τα συστήματα διανομής χαμηλής τάσης κι από τα κέντρα ελέγχου των αρχών διαχείρισης ενέργειας έως τα μικροδίκτυα χαμηλής τάσης των τελικών χρηστών.

Επιπλέον, μεταβαίνει από τις μαζικές αγορές ενέργειας σε τοπικούς παρόχους και από τους ενεργειακούς πόρους του παρελθόντος στην κατανεμημένη και ανανεώσιμη παραγωγή και αποθήκευση του παρόντος και του μέλλοντος.

Η μετάβαση από το παραδοσιακό δίκτυο σε ένα έξυπνο συνοδεύεται από αρκετές βασικές διαφορές. Αυτά περιλαμβάνουν μια μετατόπιση από τους κεντρικούς σε κατανεμημένους πόρους, μια αλλαγή από τις σαφείς κατευθύνσεις ροής ενέργειας σε απρόβλεπτες και μη γραμμικές και έναν μετασχηματισμό από ένα παθητικό σε ένα ενεργό δίκτυο. Ουσιαστικά, αυτές οι αλλαγές θα κάνουν το δίκτυο πιο δυναμικό στη διαμόρφωση και τις λειτουργίες του, ενισχύοντας τελικά την αποτελεσματικότητά του.

Εικόνα 50: Διαφορές μεταξύ Έξυπνου και υπάρχοντος Δικτύου

Παραδοσιακό Δίκτυο	Έξυπνο Δίκτυο
Συγκεντρωτική μορφή Παραγωγής	Αποκεντρωμένη Παραγωγή
Κάθετη και μονοσήμαντη ροή Ενέργειας	Διαδραστικές σχέσεις για τη ροή της Ενέργειας
Συνδέσεις Ελέγχος Παρόχου	Συμμετοχή- Έλεγχος από κάθε κόμβο-συμμετέχοντα
Συμπεριφορά, ελεγχόμενη	Συμπεριφορά, απρόβλεπτη- χαοτική

3.6 Οι προκλήσεις στα Έξυπνα Δίκτυα

Όπως αναφέρθηκε προηγουμένως στην ανάλυση των χαρακτηριστικών και των πλεονεκτημάτων των Έξυπνων Δικτύων, είναι απαραίτητη η αναβάθμιση του τρέχοντος ηλεκτρικού δικτύου μέσω της εφαρμογής αυτοματισμών, των συσκευών ελέγχου και των προηγμένων τεχνολογιών των επικοινωνιών. Αυτή είναι αναγκαία για την αντιμετώπιση διαφόρων προκλήσεων, όπως διάφορα τεχνικά ζητήματα, ξεπερασμένες υποδομές, απαιτήσεις των καταναλωτών και τη προώθηση της φιλικής προς το περιβάλλον παραγωγής ηλεκτρικής ενέργειας. Αυτά τα ζητήματα παρουσιάζονται παρακάτω εκτενέστερα.[73]

- Προκλήσεις υποδομής: Μέχρι τώρα, η υποδομή μεταφοράς ηλεκτρικής ενέργειας έχει υποστεί σημαντική φθορά λόγω των στοιχείων της. Επιπλέον, οι αυξανόμενες απαιτήσεις φορτίου περιπλέκουν περαιτέρω την κατάσταση. Τα αναδυόμενα εργαλεία της πληροφορικής, δηλαδή η ανάλυση δεδομένων και της τεχνητής νοημοσύνης, όπως η μηχανική μάθηση, που επιτρέπουν τη σύγχρονη παρακολούθηση των μετρήσεων, τον έλεγχο και την άμεση ανάδραση, είναι ζωτικής σημασίας για τη διατήρηση σταθερών δικτύων. Ωστόσο, είναι αβέβαιο εάν αυτές οι τεχνολογικές εξελίξεις θα ενισχύσουν την ανθεκτικότητα και την αξιοπιστία των συστημάτων, καθώς η πολυπλοκότητά τους μπορεί να τα κάνει πιο επιρρεπή σε κακόβουλες ενέργειες ή συχνή αποσταθεροποίηση εάν ο έλεγχος γίνει υπερβολικά αυστηρός στην ανίχνευση ψευδών σημάτων.
- Καινοτόμες τεχνολογίες: Οι ανάγκες που δημιουργούνται από τα Smart Grids προχωρούν ταχύτερα από την έρευνα και την εφαρμογή προηγμένων υλικών και τεχνολογιών. Αυτά τα υλικά και οι τεχνολογίες δεν είναι ακόμη διαθέσιμα για την επόμενη γενιά δικτύων και το τρέχον δίκτυο δεν μπορεί να συμβαδίσει με τις τεχνολογίες αιχμής. Επιπλέον, η ανάπτυξη και διαχείριση αυτών των τεχνολογιών εγείρει ανησυχίες σχετικά με το απόρρητο, καθώς η αμφίδρομη επικοινωνία μεταξύ του κέντρου ελέγχου, των συσκευών και των

[73] Πηγή: Cambell R, The Smart Grid : Status and Outlook, April 2018

καταναλωτών μπορεί να περιλαμβάνει την καταγραφή προσωπικών πληροφοριών που θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν για εμπορικούς σκοπούς με τρόπους που επί του παρόντος είναι άγνωστοι.

- Περιβαλλοντικές προκλήσεις: Η ανθρώπινη δραστηριότητα, ιδιατέρως δε μετά τη βιομηχανική επανάσταση, έχει αναγνωριστεί ως ο κύριος μοχλός της κλιματικής κρίσης, κυρίως λόγω της υπερβολικής απελευθέρωσης διοξειδίου του άνθρακα (CO2). Επιπλέον, η εξάρτησή μας από τα ορυκτά καύσιμα αποδεικνύεται μη βιώσιμη, θέτοντας ένα σημαντικό εμπόδιο στην τρέχουσα και μελλοντική παραγωγή ενέργειας. Επιπλέον, φυσικά φαινόμενα όπως οι σεισμοί έχουν τη δυνατότητα να προκαλέσουν σημαντική ζημιά στις υποδομές μεταφορών, ενώ η αποτελεσματική εφαρμογή των αστικών διατάξεων αποτελεί ένα ακόμη περίπλοκο ζήτημα στον χωροταξικό σχεδιασμό.
- Καταναλωτικές ανάγκες: Προκειμένου να παρέχονται υπηρεσίες υψηλής ποιότητας κατόπιν ζήτησης, είναι σημαντικό να υπάρχει εκτεταμένη αλληλεπίδραση καταναλωτών και δικτύου για την κάλυψη των ειδικών αναγκών όλων των τύπων εγκαταστάσεων, βιομηχανιών, εμπορικών καταστημάτων και νοικοκυριών. Είναι σαφές ότι η διαφάνεια στην αγορά είναι απαραίτητη προς όφελος των καταναλωτών, και αυτό απαιτεί τη θέσπιση νέων πολιτικών. Υπάρχει ανησυχία για το κόστος που σχετίζεται με αυτές τις νέες υπηρεσίες, καθώς η ανάπτυξη τεχνολογιών και η εφαρμογή του δικτύου θα απαιτήσουν σημαντικές αναβαθμίσεις σε ολόκληρη την υποδομή, από τις μονάδες παραγωγής έως τις μεμονωμένες κατοικίες. Χωρίς κατάλληλα μέτρα για τη στήριξη των οικονομικά μειονεκτούντων ομάδων μέσω νομοθεσίας, η εφαρμογή του έξυπνου δικτύου μπορεί να καθυστερήσει ή ακόμα και να μην είναι εφικτή για ολόκληρο τον πληθυσμό.

3.7 Έξυπνα Δίκτυα και Οικονομικές Επενδύσεις

Τα Έξυπνα Δίκτυα διαδραματίζουν καθοριστικό ρόλο στη μετάβαση σε μία οικονομία που εκπέμπει χαμηλότερο διοξείδιο του άνθρακα δημιουργώντας ένα δίκτυο πιο αποτελεσματικό αυξάνοντας τα μερίδια των ανανεώσιμων πηγών ενέργειας. Η σημαντικότητα τους διαφαίνεται στο γεγονός ότι το διάστημα 2007 - 2020 υπήρξε αύξηση των κονδυλίων από την Ευρωπαϊκή Ένωση για την έρευνα και ανάπτυξη στον κλάδο. Οι συνολικές επενδύσεις σε Έξυπνα Δίκτυα ανέρχονται σε 3,08 δισεκατομμύρια ευρώ, με τη συνεισφορά της ΕΕ να είναι 2,32 δισεκατομμύρια ευρώ.

Τα προγράμματα από τα οποία προήλθαν οι χρηματοδοτήσεις είναι το CIP-ICT-PSP που στοχεύει στη βέλτιστη της χρήση των τεχνολογιών πληροφορικής και επικοινωνιών και του από πολίτες, κυβερνήσεις και επιχειρήσεις, ιδίως τις μικρές και μεσαίες. Το CIP-IEE προωθεί την αποδοτικότερη και ορθολογική χρήση των ενεργειακών πόρων με την χρήση ανανεώσιμων πηγών δίνοντας κίνητρα για την υιοθέτηση τους από τους εμπλεκόμενους τομείς της κλιματικής κρίσης, όπως φερειπείν στις μεταφορές. Το Seventh Framework Programme (FP7) επιδιώκει την ενίσχυση της βιομηχανικής ανταγωνιστικότητας και για την κάλυψη των ερευνητικών αναγκών σε τομείς όπως η γεωργία, αλιεία, εκπαίδευση, κατάρτιση, ανταγωνιστικότητα και καινοτομία, βιομηχανία, απασχόληση και περιβάλλον.[74] Το πρόγραμμα Horizon 2020 (H2020) είναι ένα πρόγραμμα που σκοπεύει να

[74] Πηγή: Seventh framework programme of the European Community for research and technological development including demonstration activities (FP7), 2015

εξασφαλίσει την ανταγωνιστικότητα της Ε.Ε. απέναντι στο διεθνή ανταγωνισμό με γνώμονα τη βιώσιμη ανάπτυξη. Πιο συγκεκριμένα, για το διάστημα 2007 - 2020 υπήρξε αύξηση 117% στη χρηματοδότηση της Ε.Ε., αύξηση 59% στις συνολικές επενδύσεις και κατά 25% στον αριθμό των έργων, συγκριτικά με το διάστημα 2007 – 2013.[75] Το δεκαετές πρόγραμμα TYNDP 2022 του Ευρωπαϊκού Οργανισμού Διαχειριστών (ENTSOe) έχει θέσει στόχο έως το 2030 το 48% με 58% της ζήτησης του δικτύου των κρατών - μελών να καλύπτεται από ανανεώσιμες πηγές ενέργειας, με επακόλουθο τη μείωση των εκπομπών διοξειδίου του άνθρακα από 65% έως 75%, σε σύγκριση με τα επίπεδα του 1990. Περιλαμβάνει 166 projects σε δίκτυα μεταφοράς ηλεκτρικού ρεύματος και 20 projects για την αποθήκευση ενέργειας. Οι επενδύσεις για το συγκεκριμένο πρόγραμμα ανέρχονται σε 114 δισεκατομμύρια ευρώ ενώ οι ετήσιες αποσβέσεις μετά την ολοκλήρωση του υπολογίζονται από 2 έως 5 δισεκατομμύρια ευρώ.[76]

Υπάρχουν σημαντικές διαφορές μεταξύ των χωρών της ΕΕ, με την Ισπανία, τη Γερμανία και την Ιταλία να παρουσιάζουν τους μεγαλύτερους αριθμούς συμμετοχών (ορίζεται μία συμμετοχή ως συμμετοχή ενός οργανισμού σε ένα έργο) σε έργα έξυπνων δικτύων ενώ η εικόνα είναι αρκετά διαφορετική σε περιφερειακό επίπεδο, με τις πέντε κορυφαίες περιφέρειες της ΕΕ, να βρίσκονται στη Γαλλία, στην Ισπανία, στην Ελλάδα και στο Βέλγιο.

Στην Ελλάδα, ο ΔΕΔΔΗΕ έχει ήδη προκηρύξει τον διαγωνισμό για την αντικατάσταση των αναλογικών ρολογιών και την εγκατάσταση έξυπνων μετρητών, που εκτιμάται ότι θα κοστίσει 830 εκατ. ευρώ. Το σχέδιο είναι να εγκατασταθούν 7.354.000 έξυπνοι μετρητές έως το 2030. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η επένδυση αυτή θα αποσβεστεί σε λίγα χρόνια, καθώς η εισαγωγή των «έξυπνων» μετρητών θα φέρει σημαντικά πλεονεκτήματα τόσο για τους καταναλωτές όσο και για το δίκτυο διανομής. Σύμφωνα με τα στοιχεία του ΔΕΔΔΗΕ, τα οφέλη θα αυξάνονται όσο προχωρά το έργο και μέχρι το 2031 το ετήσιο όφελος αναμένεται να φτάσει τα 223 εκατ. ευρώ.[77]

[75] Πηγή: Covrig Laura, 2011
[76] Πηγή: Dimitrios Chaniotis, Laurent Schmitt, Connecting Europe: Electricity, Entso-e, 2018
[77] Πηγή: Σταύρος Γριμάνης, ΔΕΔΔΗΕ: Πώς θα τρέξει το megaproject των «έξυπνων μετρητών», Newmoney, 2022

Εικόνα 51: Επενδύσεις της Ε.Ε. στα Έξυπνα Δίκτυα

Πηγή: Joint Research Centre, 2021

Πέρα από τα οφέλη στον πάροχο ενέργειας, τα Έξυπνα Δίκτυα δημιουργούν νέες θέσεις εργασίες για εξειδικευμένο προσωπικό. Στις ΗΠΑ, για το 2008 δημιουργήθηκαν 280.000 θέσεις εργασίας, εκ των οποίων οι 140.000 αποτελούν μόνιμες θέσεις για την συντήρηση και υποστήριξη του έξυπνου δικτύου.

3.8 Νομικό Πλαίσιο της Ευρωπαϊκής Ένωσης για τα Έξυπνα Δίκτυα και τους μετρητές

Οι κανόνες της Ευρωπαϊκής Ένωσης διασφαλίζουν την προστασία των προσωπικών δεδομένων των καταναλωτών κατά την επεξεργασία και τη διακίνηση δεδομένων. Τα έξυπνα δίκτυα και οι μετρητές ενδέχεται να επηρεάσουν τα προσωπικά δεδομένα και το απόρρητο, ωθώντας την Ευρωπαϊκή Ένωση να εφαρμόσει διάφορα μέτρα για την τήρηση των κανονισμών προστασίας δεδομένων.[78]

Ένα παράδειγμα είναι το υπόδειγμα εκτίμησης επιπτώσεων που ενημερώθηκε από την Smart Grids Task Force τον Σεπτέμβριο του 2018 και το οποίο χρησιμεύει ως καθοδήγηση για την προστασία δεδομένων και το απόρρητο για τους υπεύθυνους επεξεργασίας δεδομένων και τους επενδυτές σε έξυπνα δίκτυα.[79]

Εκτός από την προστασία δεδομένων και το απόρρητο, η κυβερνοασφάλεια αναδεικνύεται ολοένα και περισσότερο σε θέμα που σχετίζεται με τα Έξυπνα Δίκτυα και τους μετρητές. Η Ευρωπαϊκή Επιτροπή δεσμεύεται να μετριάσει τυχόν κινδύνους και να ενισχύσει την ανθεκτικότητα της ασφάλειας στον κυβερνοχώρο.

[78] Πηγή: https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters_el#data-protection

[79] Πηγή: https://energy.ec.europa.eu/system/files/2018-09/dpia_for_publication_2018_0.pdf

Παρακάτω παρουσιάζονται μέρη της οδηγίας 2012/27/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2012. Προκειμένου να διασφαλιστεί η επίτευξη των πρωταρχικών της στόχων της Ευρωπαϊκής Ένωσης για αύξηση ενεργειακής απόδοσης κατά 20% το 2020 και τουλάχιστον κατά 32,5% το 2030 και να προετοιμαστεί ο δρόμος για ακόμα περισσότερες βελτιώσεις της απόδοσης μετά από αυτές τις ημερομηνίες, η παρούσα οδηγία θέτει κοινό πλαίσιο μέτρων καθιστώντας δυνατή την προώθηση της ενεργειακής πολιτικής.[80]

3.8.1 Άρθρο 9 της 2012/27/ΕΕ για τους Έξυπνους Μετρητές

Τα κράτη μέλη διασφαλίζουν ότι, εφόσον είναι τεχνικά εφικτό, οικονομικά εύλογο και ανάλογο προς τη δυνητική εξοικονόμηση ενέργειας, παρέχονται σε ανταγωνιστικές τιμές στους τελικούς καταναλωτές φυσικού αερίου, ηλεκτρικής ενέργειας, τηλεψύξης ή τηλεθέρμανσης και ζεστού νερού οικιακής χρήσης, ατομικοί μετρητές οι οποίοι καταγράφουν με ακρίβεια την πραγματική κατανάλωση ενέργειας των τελικών καταναλωτών και συγκεντρώνουν πληροφορίες σχετικά με τις πραγματικές ώρες χρήσης.

Επιπλέον, παρόμοιοι ατομικοί μετρητές θα παρέχονται πάντα στις ακόλουθες περιπτώσεις:

α) Ο υφιστάμενος μετρητής αντικαθίσταται, εκτός εάν αυτό είναι τεχνικά αδύνατο ή μη οικονομικά αποδοτικό σε σχέση με το εκτιμώμενο μακροπρόθεσμο δυναμικό εξοικονόμησης ενέργειας.

β) Σύμφωνα με την οδηγία 2010/31/ΕΕ, πραγματοποιούνται νέες συνδέσεις σε νέα κτίρια ή σε κτίρια που υποβάλλονται σε σημαντική ανακαίνιση.

Όταν χρησιμοποιούνται συστήματα έξυπνης μέτρησης σύμφωνα με τις οδηγίες 2009/72/ΕΚ και 2009/73/ΕΚ και οργανώνονται εγκαταστάσεις έξυπνων μετρητών φυσικού αερίου ή και ηλεκτρικής ενέργειας από τα κράτη μέλη τότε αυτά:

α) Εξασφαλίζουν ότι το σύστημα μέτρησης παρέχει πληροφορίες χρήσης σε πραγματικό χρόνο στους τελικούς χρήστες και ότι οι στόχοι ενεργειακής απόδοσης και τα οφέλη των τελικών χρηστών λαμβάνονται υπόψη πλήρως κατά τον καθορισμό των υποχρεώσεων που επιβάλλονται στους συμμετέχοντες στην αγορά αλλά και των ελάχιστων λειτουργιών των μετρητών.

β) Προνοούν για την ασφάλεια των έξυπνων μετρητών και της διακίνησης κι ανταλλαγής των δεδομένων τους, καθώς και την προστασία των δεδομένων προσωπικού χαρακτήρα και του απορρήτου των τελικών καταναλωτών, σύμφωνα με τη σχετική Ευρωπαϊκή νομοθεσία περί προστασίας δεδομένων και ιδιωτικότητας.

γ) Αναφορικά με την ηλεκτρική ενέργεια, απαιτούν από τον διαχειριστή του μετρητή να διασφαλίζουν ότι ο μετρητής ή οι μετρητές δύνανται να λαμβάνουν υπόψη την ηλεκτρική ενέργεια που παρέχεται στο δίκτυο από τις εγκαταστάσεις του τελικού πελάτη κατόπιν αιτήματός του.

δ) Εφόσον το ζητά ο τελικός πελάτης, να καθίστανται διαθέσιμα δεδομένα μέτρησης σχετικά με την παραγωγή ή την κατανάλωση ηλεκτρικής ενέργειας του τελικού πελάτη σε εύκολα κατανοητή μορφή, ώστε εκείνος ή τρίτος που ενεργεί για λογαριασμό του να μπορεί να τα χρησιμοποιήσει για να συγκρίνει παρόμοιες ανταγωνιστικές προσφορές.

[80] Πηγή: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:02012L0027-20210101&from=CS#tocId2

ε) Απαιτούν να παρέχονται στους καταναλωτές, κατά την εγκατάσταση του έξυπνου μετρητή, κατάλληλες συμβουλές και πληροφορίες, ιδίως σχετικά με όλες τις δυνατότητες χρήσης των ενδείξεων του μετρητή και παρακολούθησης της ενεργειακής τους κατανάλωσης.

Τέλος, εγκατάσταση εξοπλισμού μέτρησης ο οποίος μετρά την κατανάλωση ζεστού νερού χρήσης ή θερμότητας στο σημείο διανομής ή στον εναλλάκτη θερμότητας, εάν η θέρμανση, η ψύξη ή το ζεστό νερό χρήσης του κτιρίου παρέχονται από κεντρική πηγή που εξυπηρετεί πολλά κτίρια ή από δίκτυο τηλεθέρμανσης.

3.8.2 Άρθρο 10 της 2012/27/ΕΕ για την Τιμολόγηση κατανάλωσης από τους Έξυπνους Μετρητές

Όταν ο τελικός πελάτης δε διαθέτει έξυπνομετρητή όπως αναφέρεται στην οδηγία 2009/73/ΕΚ, τα κράτη μέλη διασφαλίζουν, εφόσον είναι οικονομικά δικαιολογημένο και τεχνικά εφικτό, ότι οι πληροφορίες για τις τιμές του φυσικού αερίου (ή της ηλεκτρικής ενέργειας) είναι αξιόπιστες, ακριβείς και βασίζονται στην πραγματική κατανάλωση, το αργότερο έως τις 31 Δεκεμβρίου 2014 (βλέπε παράρτημα VII στο σημείο 1.1). Η υποχρέωση αυτή δύναται να εκπληρώνεται με ένα σύστημα τακτικών μετρήσεων από τον τελικό καταναλωτή, για το οποίο εκείνος θα πρέπει να ενημερώνει τον προμηθευτή ενέργειας. Μόνο σε περίπτωση μη ενημέρωσης τα αποτελέσματα αυτής της ανάγνωσης του μετρητή για το ανάλογο χρονικό διάστημα, το τιμολόγιο θα βασίζεται σε αποδιδόμενη ή κατ' αποκοπήν κατανάλωση.

Όπως ορίζει η οδηγία 2009/73/ΕΚ οι έξυπνοι μετρητές που εγκαθίστανται προσφέρουν τη δυνατότητα ακριβούς τιμολόγησης βάσει της πραγματικής κατανάλωσης. Τα κράτη μέλη εξασφαλίζουν ότι οι τελικοί πελάτες έχουν εύκολη πρόσβαση σε συμπληρωματικές πληροφορίες που τους επιτρέπουν να επαληθεύουν το δικό τους λεπτομερές ιστορικό κατανάλωσης.

Στις πρόσθετες πληροφορίες που αφορούν το ιστορικό κατανάλωσης συγκαταλέγονται:

α) Αθροιστικά στοιχεία τουλάχιστον για τατελευταία τρία έτη ή για την περίοδο από την έναρξη της σύμβασης προμήθειας (εάν αυτή είναι μικρότερη). Τα δεδομένα αυτά θα πρέπει να αντιστοιχούν στην περίοδο για την οποία είναι συχνά διαθέσιμες πληροφορίες για τα τιμολόγια.

β) Λεπτομέρειες για τις ώρες χρήσης σε ημέρες, εβδομάδες, μήνες και έτη. Τα δεδομένα αυτά πρέπει να κοινοποιούνται στους τελικούς καταναλωτές μέσω της διεπαφής του έξυπνου μετρητή ή του διαδικτύου για περίοδο τουλάχιστον των τελευταίων 24 μηνών ή, εάν είναι συντομότερη, για την περίοδο από την έναρξη της σύμβασης προμήθειας.

Είτε έχουν εγκατασταθεί έξυπνοι μετρητές είτε όχι, τα κράτη μέλη:

α) Απαιτούν τα δεδομένα που αφορούν το ιστορικό χρέωσης και κατανάλωσης ενέργειας του τελικούπελάτη, εφόσον είναι διαθέσιμα, να παρέχονται στον πάροχο ενεργειακών υπηρεσιών που έχει επιλέξει ο τελικός πελάτης, κατόπιν αιτήματός του.

β) Διασφαλίζουν ότι ο τελικός πελάτης λαμβάνει ηλεκτρονικές πληροφορίες για την τιμολόγηση και τις επιλογές τιμολόγησης και, εφόσον το ζητήσει ο πελάτης, λαμβάνει σαφή και κατανοητή εξήγηση για τον τρόπο κατάρτισης του λογαριασμού, ιδιαίτερα δε, όταν ο λογαριασμός δεν βασίζεται στην πραγματική κατανάλωση.

γ) Εξασφαλίζουν ότι στο τιμολόγιο παρέχονται οι κατάλληλες πληροφορίες σύμφωνα με το παράρτημα VIII, ώστε ο τελικός καταναλωτής να έχει την πλήρη εικόνα του πιο πρόσφατου ενεργειακού κόστους.

δ) Κατόπιν σχετικού αιτήματος των τελικών καταναλωτών, δύνανται να προβλέπουν ότι οι πληροφορίες που περιέχονται στα εν λόγω τιμολόγια δε λογίζονται ως αίτημα πληρωμής. Στην περίπτωση αυτή, τα κράτη μέλη εξασφαλίζουν ότι οι προμηθευτές ενέργειας προσφέρουν ευέλικτες ρυθμίσειςπληρωμής.

ε) Δύνανται να απαιτούν να παρέχονται πληροφορίες και εκτιμήσεις του ενεργειακού κόστους κατόπιν σχετικού αιτήματος των τελικών καταναλωτών, εγκαίρως και με κατανοητό τρόπο, ώστε να έχουν την δυνατότητα οι τελευταίοι να συγκρίνουν ανταγωνιστικές προσφορές.

3.8.3 Τα Άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων περί Προστασίας Ιδιωτικότητας και Προσωπικών Δεδομένων

Με τη χρήση των SmartGrids στο ηλεκτρικό δίκτυο δημιουργείται η ανάγκη για την προστασία των δεδομένων των χρηστών, καθώς ο πάροχος ηλεκτρικής ενέργειας έχει πρόσβαση σε ευαίσθητα προσωπικά δεδομένα. Η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων αποτελούν θεμελιώδες δικαίωμα της ΕΕ.

Σε μια κλασική διατύπωση, «η ιδέα της ιδιωτικής ζωής περιλαμβάνει την επιθυμία να μείνουμε μόνοι, ελεύθεροι να είμαστε ο εαυτός μας – ανεμπόδιστοι και απεριόριστοι από τα αδιάκριτα των άλλων» (Wacks, 2010, σ. 30). Καθώς ωρίμαζε η σύλληψη της ιδιωτικής ζωής, κατέστη σαφές ότι μία από τις πτυχές αυτού του «μένουν μόνοι», δηλαδή αυτή που αφορά πληροφορίες που σχετίζονται με ένα άτομο, άμεσα ή έμμεσα, απαιτεί ξεχωριστή προσοχή. Με άλλα λόγια, δημιουργήθηκε η έννοια της «προστασίας δεδομένων».[81] Ο Χάρτης των Θεμελιωδών Δικαιωμάτων έχει αναγνωρίσει ρητά το απόρρητο και την προστασία των προσωπικών δεδομένων ως δύο ξεχωριστά αλλά αλληλένδετα δικαιώματα.

Στα θεμελιώδη ανθρώπινα δικαιώματα και στο Άρθρο 7 η ΕΕ διασφαλίζει το σεβασμό της ιδιωτικής και οικογενειακής ζωής. Από το άρθρο απορρέει ότι κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της κατοικίας του και των επικοινωνιών του, αλλά και της ιδιωτικής και οικογενειακής ζωής του.

Στο Άρθρο 8 για την Προστασία των δεδομένων προσωπικού χαρακτήρα[82] αναφέρεται ότι:

1. Ο καθένας έχει το δικαίωμα να προστατεύονται τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν.
2. Τα δεδομένα αυτά πρέπει να υποβάλλονται σε νόμιμη επεξεργασία για συγκεκριμένο σκοπό, βάσει της συγκατάθεσης του ενδιαφερόμενου προσώπου ή για άλλους απαραίτητους λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει το δικαίωμα να έχει πρόσβαση στα δεδομένα που συλλέγονται για το ίδιο και να έχει τη δυνατότητα διόρθωσής τους.
3. Η τήρηση του παρόντος κανονισμού υπόκειται στον έλεγχο ανεξάρτητης αρχής.

[81] Πηγή: De Hert&Gutwirth, 2009; Finn et al., 2013; Gellert&Gutwirth, 2013; González Fuster, 2014; Kokott&Sobotta, 2013

[82] Πηγή: http://fra.europa.eu/el/eu-charter/article/8-prostasia-ton-dedomenon-prosopikoy-haraktira

3.9 Στόχοι Κυβερνοασφάλειας

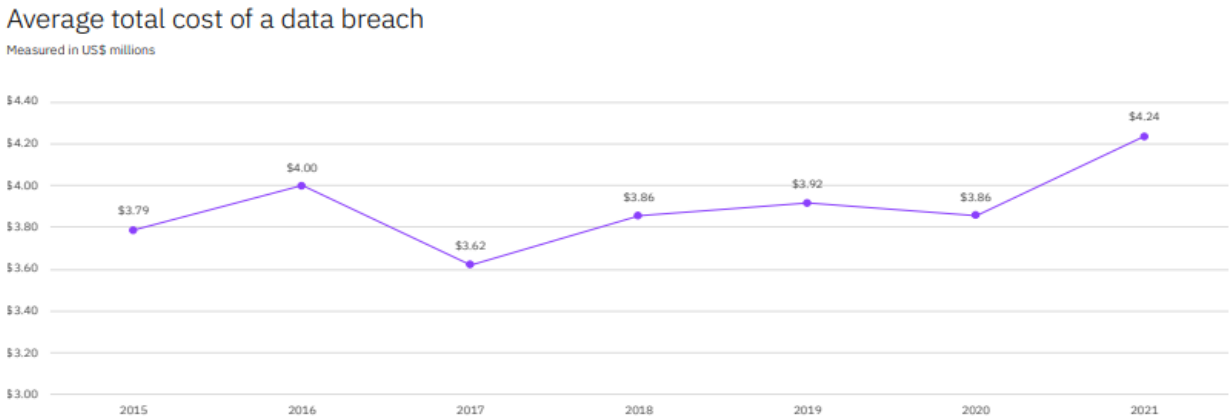
Τα παραδοσιακά δίκτυα παροχής ηλεκτρικού ρεύματος εξελίσσονται στα Έξυπνα Δίκτυα παροχής ηλεκτρικής ενέργειας. Ένα Έξυπνο Δίκτυο εμπλουτίζει στην ουσία το παραδοσιακό δίκτυο με τις Τεχνολογίες Πληροφορικής κι Επικοινωνιών (ICT). Αυτή η μετάβαση βελτιώνει την αποδοτικότητα και τη διαθεσιμότητα της ηλεκτρικής ενέργειας από τους παρόχους στους καταναλωτές, καθώς η επίβλεψη, ο έλεγχος και η διαχείριση της ζήτησης του αγαθού από τους πελάτες είναι πιο ακριβής από ποτέ. Πρέπει να εξετάζονται οι κύριες ευπάθειες του Έξυπνου Δικτύου, ο προσδιορισμός των επιτιθέμενων, τα είδη των επιθέσεων, και οι απαιτούμενες λύσεις. Οι κύριοι στόχοι ασφάλειας που πρέπει να ενσωματωθούν στα έξυπνα δίκτυα είναι οι εξής:

1) Διαθεσιμότητα αδιάκοπης παροχής ηλεκτρικού ρεύματος σύμφωνα με τη ζήτηση του χρήστη.
2) Ακεραιότητα των πληροφοριών που διακινούνται στο δίκτυο.
3) Εμπιστευτικότητα των δεδομένων του χρήστη.
4) Προληπτική ανάλυση. Σε αντίθεση με τα κλασικά συστήματα IT, σε μία τόσο κρίσιμη υποδομή όπως τα Έξυπνα Δίκτυα, η αντιδραστική ασφάλεια χρησιμοποιώντας απόκριση απειλών για τη μείωση της ζημιάς δεν αρκεί. Οπότε απαιτείται από πριν ανάλυση για εντοπισμό πιθανών απειλών ώστε να εξαλειφθεί ο παραμικρός χώρος για επίθεση στο έξυπνο δίκτυο και να αποφευχθούν επιζήμιες συνέπειες.
5) Αυτοματοποίηση της ανάλυσης ασφαλείας για τα μεγάλα και υβριδικά συστήματα όπως τα Έξυπνα Δίκτυα. Οι οδηγίες ασφαλείας που αναπτύχθηκαν από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Η.Π.Α. (NIST) είναι εξαιρετικά λεπτομερείς.
6) Δραστικά μέτρα ασφάλειας, δηλαδή η δυνατότητα παροχής ασφάλειας και ανθεκτικότητας στα Έξυπνα Δίκτυα, εισάγοντας εγρήγορση στις ιδιότητες του συστήματος.

3.10 Το κόστος των Κυβερνοεπιθέσεων και οι πολιτικές για την Κυβερνοαφάλεια

Τα κυβερνοεγκλήματα κοστίζουν στην παγκόσμια οικονομία πάνω από 575 δισεκατομμύρια δολάρια κάθε χρόνο (Sobers, 2019). Καθώς η χρήση του διαδικτύου είναι απαραίτητη στην καθημερινότητα μας, με ολοένα και περισσότερους χρήστες να έχουν πρόσβαση στο ίντερνετ, υπάρχει μία ιδιαίτερη ανησυχία όσον αφορά τις κυβερνοεπιθέσεις. Το πιο πιθανό είναι ότι το κόστος από τις κυβερνοεπιθέσεις θα συνεχίσει να αυξάνεται καθώς όλο και περισσότερες επιχειρήσεις κινούνται προς τη ψηφιοποίηση των διαδικασιών τους αυξάνοντας τη χρήση του διαδικτύου και τη σύνδεση τους με υπηρεσίες Cloud. Σύμφωνα με την IBM, οι παραβιάσεις των προσωπικών δεδομένων αυξήθηκαν κατά 10% το διάστημα 2020 - 2021. Με βάση τα δεδομένα που έλαβε η εταιρία από 537 οργανισμούς από 17 διαφορετικές χώρες και βιομηχανίες, υπολόγισε το μέσο κόστος από τη διαρροή δεδομένων. Είναι αξιοσημείωτο ότι από το 2015, το κόστος αυξήθηκε κατά 11,90%, δηλαδή 0,45 εκατομμύρια δολάρια.

Εικόνα 52: Το κόστος των Κυβερνοεπιθέσεων



Πηγή: https://www.ibm.com/security/data

Τα Έξυπνα Δίκτυα θα αποτελέσουν σημαντική επένδυση στα ηλεκτρικά δίκτυα των σύγχρονων οικονομιών, απαιτώντας ειδικές ενέργειες Κυβερνοασφάλειας για τον εντοπισμό, την προστασία και την ανάκτηση του δικτύου από κυβερνοεπιθέσεις και την αποφυγή ή τον μετριασμό της διακοπής ρεύματος ή τα προβλήματα στην ποιότητα του ρεύματος και τις διακοπές υπηρεσιών, συμπεριλαμβανομένων των λειτουργιών κατά τη διάρκεια μιας κυβερνοεπίθεσης. Τα κόστη από μία κυβερνοεπίθεση μπορούν να είναι άμεσα ή έμμεσα. Στα άμεσα κόστη περιλαμβάνονται η διακοπή στο δίκτυο, αντικατάσταση ή αναβάθμιση κατεστραμμένου εξοπλισμού, η διαρροή προσωπικών δεδομένων, η δυσφήμιση της εταιρείας παροχής ρεύματος, κλπ.

Ενδεικτικά, το πιο σημαντικό είδος λυτρισμικού (ransomware) είναι το «CryptoLocker» το οποίο διαδίδεται ως συνημμένο σε email. Εκτιμάται ότι το «CryptoLocker» μόλυνε περίπου 234.000 υπολογιστές, αποσπώντας περισσότερα από 27 εκατομμύρια δολάρια τους πρώτους δύο μήνες λειτουργίας του (ΟΟΣΑ, 2015). Επιπλέον, η σοβαρότητα και η συχνότητα των επιθέσεων κακόβουλου λογισμικού παρουσιάζουν μια ανοδική τάση. Σε μια εβδομάδα ένας οργανισμός μπορεί να λάβει κατά μέσο όρο σχεδόν 17.000 κακόβουλες ειδοποιήσεις. Ο χρόνος απάντησης σε αυτές τις ειδοποιήσεις είναι μια σοβαρή εξάντληση των οικονομικών πόρων ενός οργανισμού και του προσωπικού ασφάλειας πληροφορικής. Το μέσο κόστος του χρόνου που χάνεται για την απάντηση σε ανακριβή και εσφαλμένη νοημοσύνη μπορεί να είναι κατά μέσο όρο 1,27 εκατομμύρια δολάρια ετησίως. Από αυτές τις 17.000 ειδοποιήσεις μόνο το 19% θεωρείται αξιόπιστο και μόνο το 4% διερευνάται.

Τον Ιούνιο του 2021, το US Department of Energy, δημιούργησε ένα εργαλείο για τους παρόχους ηλεκτρικής ενέργειας, προκειμένου να αξιολογήσουν και να βελτιώσουν την ικανότητα τους να αμυνθούν σε μελλοντικές κυβερνοεπιθέσεις. Το DoE ανακοίνωσε την κυκλοφορία του Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2), μέρος ενός σχεδίου της κυβέρνησης Μπάϊντεν για την αντιμετώπιση απειλών στον κυβερνοχώρο σε κρίσιμα συστήματα που είναι απαραίτητα για την εθνική και οικονομική ασφάλεια των ΗΠΑ.[83] Το C2M2, το οποίο κυκλοφόρησε για πρώτη φορά το 2012, έχει σχεδιαστεί για να βοηθήσει τους

[83] Πηγή: Magill, 2021

οργανισμούς στον ενεργειακό τομέα να κατανοήσουν τους κινδύνους στον κυβερνοχώρο για τα συστήματα τεχνολογίας πληροφοριών. Το ενημερωμένο μοντέλο περιλαμβάνει στοιχεία από 145 ειδικούς στον τομέα της Κυβερνοασφάλειας που εκπροσωπούν 77 οργανισμούς του ενεργειακού τομέα. Τον Αύγουστο του ίδιου έτους, η κυβέρνηση ανακοίνωσε ότι θα δοθούν 2 δισεκατομμύρια δολάρια τα οποία προορίζονται για τη βελτίωση σε ένα ευρύ φάσμα συστημάτων Κυβερνοασφάλειας.

3.11 Βασικές Επιθέσεις στα Έξυπνα Δίκτυα

Οι παρακάτω προτάσεις είναι πιθανές κοινές απειλές που πρωτοεμφανίστηκαν στον χώρο των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ), οι οποίες δύνανται να προκαλέσουν μεγάλες ζημιές στα Έξυπνα Δίκτυα. Αυτοί οι κίνδυνοι καθίστανται ιδιαίτερα επιζήμιοι από την ιδιωτικότητα των ατόμων, όπως τα ευαίσθητα δεδομένα των καταναλωτών, το ρίσκο κλοπής πληροφοριών ως ακόμα και τον τερματισμό μίας ολόκληρης επιχείρησης. Επιπλέον, οι κίνδυνοι αυτοί δεν περιορίζονται στην αλληλεπίδραση με το διαδίκτυο, όπως οι κλασικές απειλές, αλλά επηρεάζουν και τους οικιακούς πελάτες καθώς οι επιτιθέμενοι θα μπορούσαν να συγκεντρώσουν πολύτιμες προσωπικές πληροφορίες όπως την ταυτότητα, τη χρήση των υπηρεσιών, τις προτιμήσεις και τις συνήθειες τους.[84] Παρακάτω παρουσιάζονται αναλυτικά:

3.11.1 Ηλεκτρονικό Ψάρεμα (Phishing)

Το ηλεκτρονικό ψάρεμα θα μπορούσε να είναι το πρώτο βήμα έκθεσης πελατών και οργανισμών σε κίνδυνο, καθώς η διεκπεραίωση του είναι αρκετά εύκολη. Οι επιτιθέμενοι θα μπορούσαν να χρησιμοποιήσουν πληροφορίες των καταναλωτών, αν αποκτούσαν πρόσβαση στους ηλεκτρικούς λογαριασμούς ή τις αποδείξεις πληρωμής τους. Στη συνέχεια, αξιοποιώντας τα παραπάνω και παριστάνοντας τους καταναλωτές χρησιμοποιώντας την επονομαζόμενη «κοινωνική μηχανική» (social engineering) θα μπορούσαν να αποκτήσουν κομβικής σημασίας πληροφορίες για τους καταναλωτές ή τον οργανισμό τους και τον αντίστοιχο πάροχο ηλεκτρικής ενέργειας. Από την άλλη μεριά, μέσα στον οργανισμό του παρόχου, ο υπεύθυνος εργαζόμενος που διαχειρίζεται τα στοιχεία των καταναλωτών θα μπορούσε να εξαπατηθεί λαμβάνοντας ψεύτικα ηλεκτρονικά μηνύματα (emails) που φαίνονται επίσημα και τα οποία θα μπορούσαν να τον οδηγήσουν να εκχωρήσει πολύτιμες πληροφορίες (όπως στοιχεία πιστωτικής κάρτας) σε λάθος χέρια, οδηγώντας σε χακάρισμα. Αυτοί οι κίνδυνοι θα μπορούσαν να βλάψουν οικονομικά και ψυχικά τους πελάτες και τα συμφέροντα των παρόχων.

3.11.2 Άρνηση της Υπηρεσίας (Denial of Service)

Η Άρνηση της Υπηρεσίας, είναι μία επίθεση στρατηγικού χαρακτήρα και κάθε απειλή, που στοχεύει στην άρνηση διαθεσιμότητας του αγαθού (εν προκειμένω της ηλεκτρικής ενέργειας) μπορεί να θεωρηθεί κομμάτι αυτού του είδους επίθεσης. Όσον αφορά τα Έξυπνα Δίκτυα, οι κυρίαρχες υπηρεσίες τους έχουν να κάνουν με διαθεσιμότητα, πράγμα που σημαίνει ότι υπάρχει πιθανότητα να συμβεί αυτή η επίθεση. Η σύνδεση συνδεσιμότητας των Έξυπνων Δικτύων πρέπει να είναι ασφαλής και αξιόπιστη. Ο λόγος που πρέπει να είναι αξιόπιστη η σύνδεση της συνδεσιμότητας είναι επειδή τα Έξυπνα Δίκτυα κατανέμουν την σύνδεση σε αμέτρητες συσκευές σε

[84] Πηγή: https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity

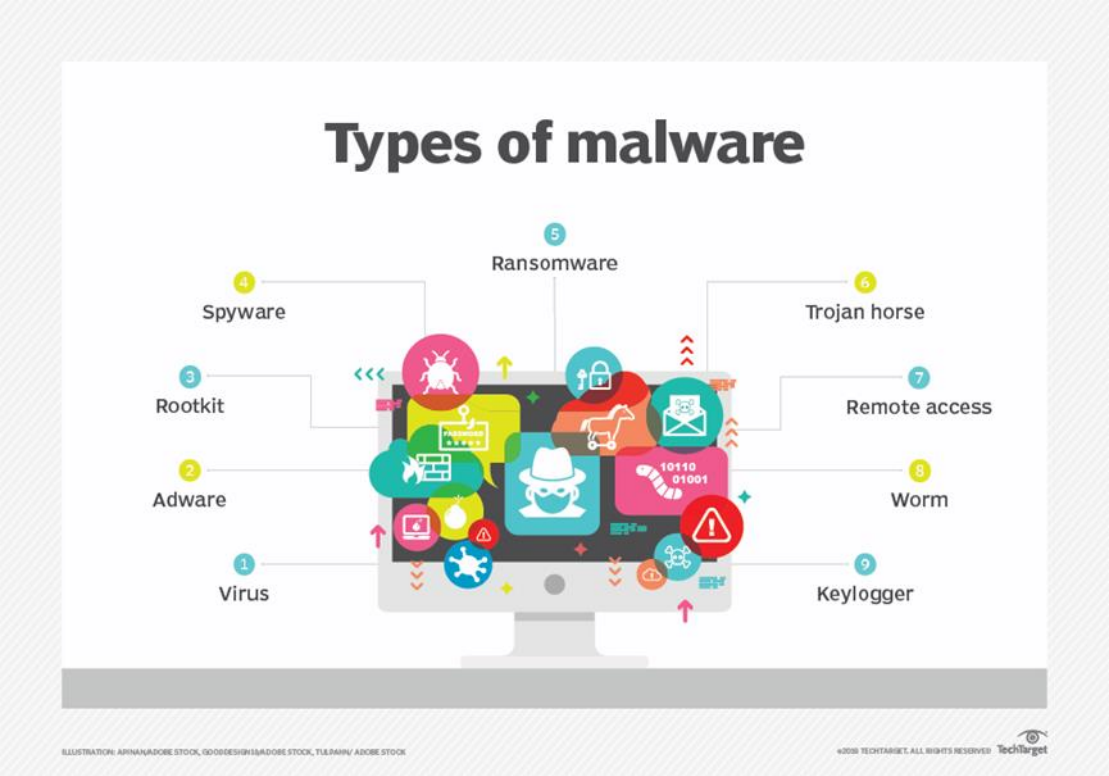
μία μεγάλη περιοχή χρησιμοποιώντας συστήματα κατανεμημένης αρχιτεκτονικής. Αν η επίθεση συνεπώς συμβεί στο έξυπνο πλέγμα, τότε η απώλεια θα είναι τεράστια. Η Άρνησης της Υπηρεσίας θα συμβεί όταν μπλοκαριστεί το κανάλι επικοινωνίας και είναι ένας κοινός τρόπος επίθεσης στο Φυσικό επίπεδο και στο επίπεδο Ζεύξης - Δεδομένων του μοντέλου OSI. Πως θα γίνει αυτό; Οι χάκερς θα μπορούσαν να τροποποιήσουν την διεύθυνση MAC (που κάθε συσκευή έχει μοναδική) με κάποιο εργαλείο όπως το Tsunami Backdoor ώστε να αποκτήσουν (backdoor) πρόσβαση στο δίκτυο και έπειτα να πλημμυρήσουν τους υπολογιστές του δικτύου με υπερβολικά αιτήματα σύνδεσης, οδηγώντας τους να χρησιμοποιήσουν όλους τους δυνατούς πόρους του υλικού τους (hardware) έως ότου καταρρεύσουν και τεθούν εκτός λειτουργίας, σταματώντας να παρέχουν τις αρχικές τους υπηρεσίες. Τα πρωτόκολλα ασφαλείας στα επίπεδα Δικτύου και Μεταφοράς του μοντέλου OSI, όπως τα TCP, SSL και IPv6 έχουν μία ασφάλεια από τη δομή τους αλλά μπορεί να είναι ευπαθή στις πρώιμες μορφές τους όταν προέρχονται από παλιές συσκευές που είναι μέρος της αρχιτεκτονικής των Έξυπνων Δικτύων. Τέλος, η επίθεση Άρνησης της Υπηρεσίας κυρίως εκτελείται στο επίπεδο Εφαρμογής του μοντέλου OSI επειδή αυτό το επίπεδο ενεργοποιεί τη μεταφορά και λήψη δεδομένων, και όσον αφορά τα Έξυπνα Δίκτυα, όταν συμβεί αυτή η επίθεση τότε μπορεί να τερματίσει την απόκριση του συστήματος επικοινωνίας προς τις διάφορες συσκευές του έξυπνου πλέγματος.[85]

3.11.3 Διαμοιρασμός Κακόβουλου Λογισμικού (Malware Spreading)

Πρόκειται για άλλον ένα μεγάλο κίνδυνο στα έξυπνα δίκτυα, που μπορεί να είναι εξαιρετικής σημασίας. Οι επιτιθέμενοι μπορούν να αναπτύξουν ποικίλους τύπους κακόβουλων λογισμικών τα οποία μπορούν να καθοδηγηθούν ώστε να μολύνουν όχι μόνο τους εξυπηρετητές (servers) του οργανισμού, αλλά και τις συσκευές που εμπλέκονται στο Έξυπνο Δίκτυο. Χρησιμοποιώντας λοιπόν το διαμοιρασμό αυτών των λογισμικών, ο επιτιθέμενος θα μπορεί να παραποιήσει τις λειτουργίες των συσκευών ή των συστημάτων έτσι ώστε να επιτρέψουν στους επιτιθέμενους να αποκτήσουν παράνομη πρόσβαση για τη συλλογή ευαίσθητων πληροφοριών. Οι κύριες κατηγορίες τους είναι στην παρακάτω εικόνα:

[85] Πηγή: https://www.aimspress.com/article/id/5ffd82bcba35de34e6cde4bd

Εικόνα 53: Είδη κακόβουλων λογισμικών



Πηγή: https://www.techtarget.com/searchsecurity/definition/malware

3.11.4 Υποκλοπή και ανάλυση κίνησης της πληροφορίας (Eavesdropping and traffic analysis)

Η υποκλοπή και η ανάλυση της κίνησης των δεδομένων είναι είδη πλαστογραφικής επίθεσης (spoofing attacks). Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε κρίσιμες πληροφορίες επιβλέποντας κι αναλύοντας μη εξουσιοδοτημένα την κίνηση των δεδομένων στο δίκτυο. Τα Έξυπνα Δίκτυα θα πρέπει να αντιμετωπίσουν αυτό το κίνδυνο επειδή το μέγεθος των δικτύων τους, οι κόμβοι και οι συσκευές που τα αποτελούν είναι τεράστια και δύσκολο να συντηρούνται και να αναβαθμίζονται, υστερώντας σε ασφάλεια. Ο μεγαλύτερος κίνδυνος κι εδώ συνεπώς είναι η κλοπή δεδομένων, άρα πρέπει να δοθεί έμφαση στην ασφάλεια τους από ολόκληρο τον κόσμο που μπορεί να έχει πρόσβαση.

3.12 Κατηγοριοποίηση των Κυβερνοεπιθέσεων στα Έξυπνα Δίκτυα

Οι επιθέσεις κατηγοριοποιούνται έχοντας λάβει υπόψη τις 3 αρχές της κυβερνοασφάλειας των IT συστημάτων, ήτοι της Εμπιστευτικότητας (Confidentiality), της Ακεραιότητας (Integrity) και της Διαθεσιμότητας (Availability). Τα αρχικά αυτών των αγγλικών όρων σχηματίζουν το περίφημο CIA. Πρώτα απ' όλα, η διαθεσιμότητα πρέπει να είναι εξασφαλισμένη καθώς τα έξυπνα δίκτυα πρέπει να παρέχουν αποδοτική χρήση της ηλεκτρικής υποδομής. Η ακεραιότητα είναι δεύτερη

στην προτεραιότητα ενώ η εμπιστευτικότητα είναι τρίτη. Ο παρακάτω πίνακας περιλαμβάνει τις επιθέσεις που παρεμποδίζουν την τριάδα CIA στα έξυπνα δίκτυα.[86]

Εικόνα 54: Ταξινόμηση των Κυβερνοεπιθέσεων στα Έξυπνα Δίκτυα

CIA	Επίθεση
Confidentiality	Social Engineering, Eavesdropping, Traffic Analysis, Unauthorized Access, Password Pilfering, MITM, Sniffing, Replay, Masquerading, Data Injection
Integrity	Tampering, Replay, Wormhole, False Data Injection, Spoofing, Data Modification, MITM, Time Synchronization, Masquerading, Load-Drop
Availability	Jamming, Wormhole, Denial of Service, LDos, Buffer Overflow, Teardrop, Smurf, Puppet, Time Synchronization, Masquerading, MITM, Spoofing

Πηγή: https://www.researchgate.net/publication/331418396_Analysis_of_cyber-attacks_on_smart_grid_applications

3.13 Παραβιάσεις Ασφαλείας – Διάσημες Κυβερνοεπιθέσεις

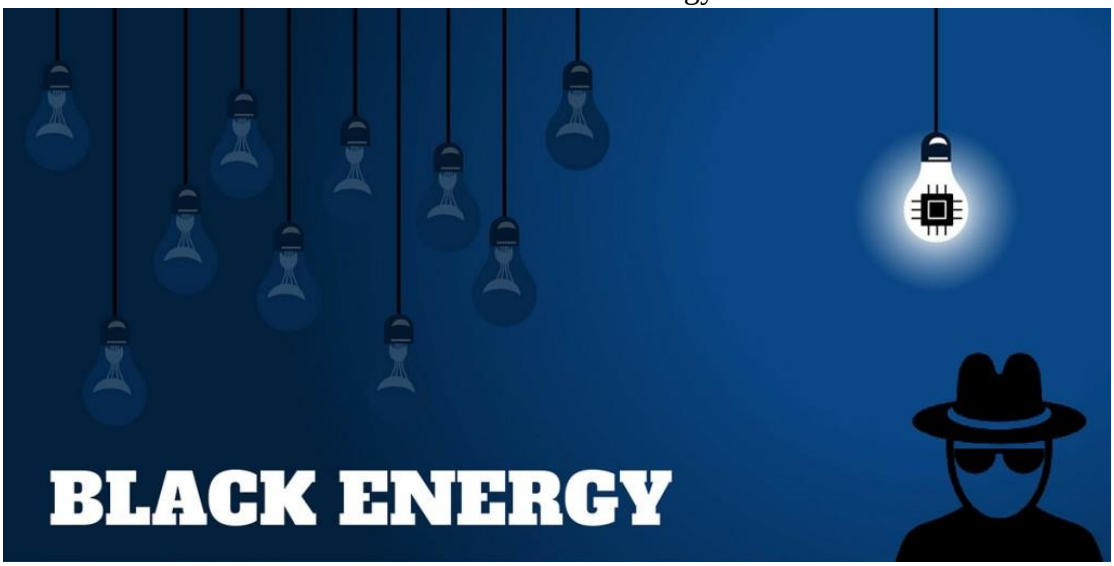
Η τεχνολογία των Έξυπνων Δικτύων Παροχής Ηλεκτρικής Ενέργειας, αποτελείται από τεχνολογίες Δικτύων και Τηλεπικοινωνιών, και εκμεταλλευόμενη τη λογική τους, προσφέρει μοναδικά οφέλη μαζί με την ενέργεια. Αυτό ωστόσο, τα καθιστά επίσης ευάλωτα και σε επιθέσεις που αφορούν τα δίκτυα υπολογιστών. Έχουν συμβεί πολυάριθμες παραβιάσεις μεγάλης εμβέλειας τα τελευταία χρόνια, των οποίων η ανάλυση και μελέτη είναι αναγκαίες, καθώς παρέχουν λύσεις για την αντιμετώπιση τους. Αναλύουμε παρακάτω τις 3 πιο διάσημες κυβερνοεπιθέσεις και πιο κοντινές στη φιλοσοφία των Έξυπνων Δικτύων και προτείνουμε λύσεις ώστε να μη ξανασυμβούν, ειδικά σε τόσο κρίσιμες υποδομές όπως αυτές που παρέχουν την πηγή ενέργειας σχεδόν όλων των συσκευών, δηλαδή του ηλεκτρισμού.

[86] Πηγή: https://www.researchgate.net/publication/331418396_Analysis_of_cyber-attacks_on_smart_grid_applications

3.13.1 Black Energy

Είδος: Τρωικό Άλογο Κακόβουλο Λογισμικό (TrojanHorseMalware)

Εικόνα 55: BlackEnergy



Πηγή: https://www.ebcg.com/wp-content/uploads/2016/03/BLACK-ENERGY-1024x512.jpg

Στον Τρωικό Πόλεμο, ο Δούρειος Ίππος παρουσιάστηκε σαν δώρο, το δέχτηκαν οι Τρώες από τους Αχαιούς, αλλά αποτέλεσε την αφορμή του ανοίγματος της κερκόπορτας για την καταστροφή της Τροίας. Κατά παρόμοιο τρόπο, ένα Trojan ή Trojan Horse μεταμφιέζεται σε ένα νόμιμο πρόγραμμα που ξεγελά το χρήστη να το κατεβάσει, εγκαταστήσει κι εκτελέσει στη συσκευή του, και το οποίο με τη σειρά του εκτελεί κακόβουλο λογισμικό. Τα Trojans είναι μία θύρα εισαγωγής στην ουσία και σε αντίθεση με τα Worms χρειάζονται ξενιστή για να λειτουργήσουν. Όταν ένα Trojan έχει εγκατασταθεί σε μία συσκευή, οι χάκερς μπορούν να το εκμεταλλευτούν έτσι ώστε να διαγράψουν, τροποποιήσουν ή συλλέξουν δεδομένα, κατασκοπεύσουν τη συσκευή, αποκτήσουν πρόσβαση στο δίκτυο της συσκευής και χρησιμοποιήσουν τη συσκευή σαν ένα συστατικό botnet, δηλαδή μέρος ενός δικτύου συσκευών καθοδηγούμενων από χάκερς για διάφορες άλλες επιθέσεις, όπως την περίφημη κατανεμημένη άρνηση υπηρεσίας (DDoS), δηλαδή αποστολή μαζικών αιτημάτων προς ένα σύστημα μέχρις ότου καταρρεύσει.[87]

Στις 25 Δεκεμβρίου 2015 μία κυβερνοεπίθεση έλαβε χώρα κατά τη διάρκεια του εμφύλιου πολέμου στην Ουκρανία. Ο στόχος ήταν ο ηλεκτροπαραγωγικός σταθμός της πόλης Ιβάνο - Φρανκίφσκ (Ivano - Frankivsk) και το αποτύπωμα της επίθεσης ήταν γιγαντιαίο καθώς 80.000 άνθρωποι κινδύνεψαν εφόσον έμειναν στο σκοτάδι, ενώ συνολικά 1.400.000 επηρεάστηκαν.

Η κυβερνοεπίθεση συνέβη χρησιμοποιώντας spear phishing email το οποίο περιείχε το Trojan κακόβουλο λογισμικό BlackEnergy. Η διαφορά με το απλό phishing, είναι ότι τα spear phishing emails είναι προσεκτικά σχεδιασμένα για συγκεκριμένα άτομα ή ομάδες που έχουν ένα συγκεκριμένο πόστο συνήθως υψηλής ευθύνης σε έναν οργανισμό.[88]

[87] Πηγή: https://www.ebcg.com/blackenergy-or-how-to-hack-an-energy-provider/

[88] Πηγή: https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing

Ο ισχυρός αυτός ιός διέγραψε δεδομένα, κατέστρεψε σκληρούς δίσκους και κατέλαβε υπό έλεγχο τους προσβεβλημένους υπολογιστές. Η επίθεση προχώρησε περαιτέρω, καθώς ο επιτιθέμενος εξαπέλυσε μία συντεταγμένη επίθεση άρνησης υπηρεσίας (Denial of Service – DoS) στον εξοπλισμό της εταιρίας, προκαλώντας ανεπανόρθωτη βλάβη στον τηλεφωνικό αριθμό υποστήριξης του ηλεκτρικού σταθμού. Εξαιτίας αυτού του γεγονότος, οι χρήστες δεν ήταν δυνατό να επικοινωνήσουν και να αναφέρουν τη βλάβη. Έτσι λοιπόν αυτή η επίθεση οδήγησε σταδιακά στην αποσταθεροποίηση μίας κρίσιμης υποδομής μίας χώρας, πέρα από το κλέψιμο των δεδομένων. Επρόκειτο για ένα από τα μεγαλύτερα πλήγματα, καθώς χωρίς ηλεκτρισμό πολλοί άνθρωποι υπέφεραν από τις εξαιρετικά χαμηλές θερμοκρασίες.

Σε αρχικό επίπεδο, παρότι η προστασία έναντι τέτοιου είδους επιθέσεων δεν μπορεί να είναι ποτέ πλήρως εγγυημένη, η πρόληψη, δηλαδή η έγκαιρη ενημέρωση καθώς και η κουλτούρα ασφαλείας προς το προσωπικό ενός οργανισμού, για τους ενδεχομένους κινδύνους που μπορεί να κρύβονται σε ένα email, μπορεί σίγουρα να μετριάσει τις πιθανότητες να συμβεί ένα παρόμοιο περιστατικό. Επιπλέον, για την αντιμετώπιση γνωστών ευπαθειών των συστημάτων πληροφορικής, από τα δίκτυα έως τις συσκευές που τα αποτελούν, συστήνεται η αναβάθμιση του εξοπλισμού και των εφαρμογών τους και η συνεχής ενημέρωση στα αντιικά προγράμματα προστασίας τους με νέες αντιικές υπογραφές (δηλαδή γνωστοποίηση των τελευταίων ιών) και σωστές ρυθμίσεις φιλτραρίσματος της κίνησης των δεδομένων από τα τείχη προστασίας (firewalls) των δρομολογητών του δικτύου. Ένα σωστά ρυθμισμένο κι ενημερωμένο firewall μπορεί να χρησιμοποιηθεί για να μπλοκάρει την εισερχόμενη κίνηση από τις συγκεκριμένες θύρες, αλλά το ίδιο δεν μπορεί να αντιμετωπίσει την περίπτωση των spear phishing emails. Τα Sandboxes, δηλαδή απομονωμένα από κεντρικά δίκτυα περιβάλλοντα δοκιμών παρέχουν προστασία κατά την εκτέλεση μη επιβεβαιωμένων εφαρμογών ή και εγγράφων.[89] Πρόκειται ουσιαστικά για ένα δοκιμαστικό λειτουργικό σύστημα, έναν εικονικό υπολογιστή στον κεντρικό υπολογιστή του χρήστη, όπου μπορεί να αναλυθεί η συμπεριφορά ενός κακόβουλου λογισμικού από ένα αρχείο, μένοντας εκεί. Με το VMware Workstation, μπορεί να δημιουργηθεί ένα σχετικό φθηνό sandbox το οποίο εκμεταλλεύεται τους πόρους του βασικού υπολογιστή (Εικόνα 56)[90]. Εάν μολυνθεί συνεπώς ο εικονικός υπολογιστής απλά τον διαγράφουμε χωρίς να επεκταθεί στο υπόλοιπο δίκτυο η μόλυνση.[91]

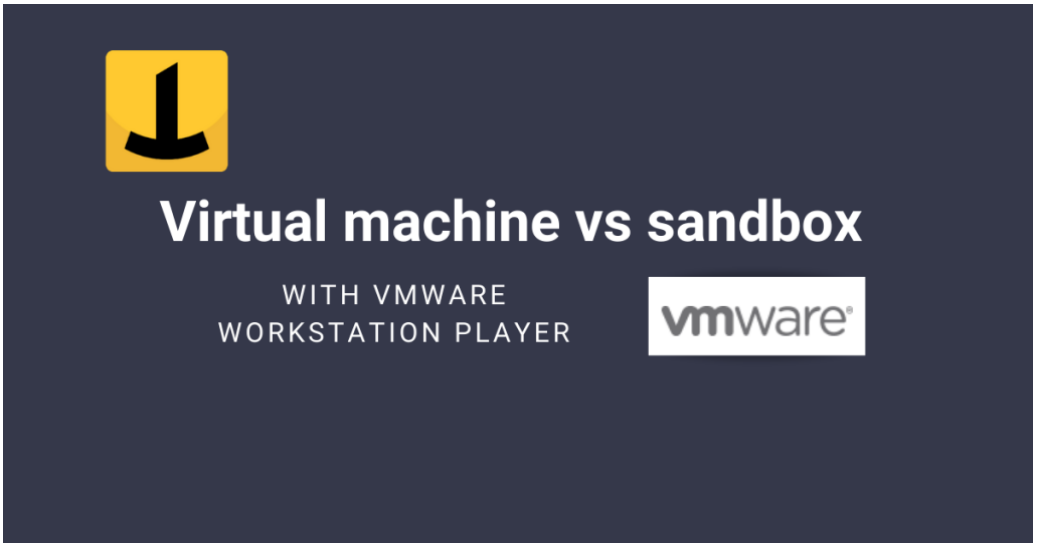
---

[89] Πηγή: https://www.techtarget.com/searchsecurity/definition/sandbox

[90] Πηγή: https://www.iperiusbackup.net/en/virtual-machines-and-sandboxes-to-use-them-within-vmware-workstation-player/

[91] Πηγή: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/86558342/Threat_Analysis_of_BlackEnergy_Malware_for_Synchrophasor_based_Real_time_Control_and_Monitoring_in_Smart_Grid.pdf

Εικόνα 56: VMWare Workstation Sandbox



Πηγή: https://www.iperiusbackup.net/en/virtual-machines-and-sandboxes-to-use-them-within-vmware-workstation-player/

Όσον αφορά τους διαχειριστές και τους χρήστες των πληροφοριακών συστημάτων, συστήνονται η πολυπαραγοντικήαυθεντικοποίηση, πχ όπως γίνεται η αυθεντικοποίηση κατά την είσοδο στους internetbanking λογαριασμούς στις ιστοσελίδες των τραπεζών, όπου χρησιμοποιείται και κωδικός που έχει σταλεί στο τηλέφωνο του χρήστη, πέραν της απλής ταυτοποίησης με username και password του, η χρήση ισχυρών κωδικών που αναλύουμε στην επόμενη ενότητα, και η τήρηση των μέτρων ασφαλείας όπως η επίβλεψη των δικτύων και των συμβάντων (logs).

3.13.2 Stuxnet

Είδος: Κακόβουλο Σκουλήκι Υπολογιστών (Computer Malicious Worm)

Εικόνα 57: Stuxnet vs Πυρηνικό πρόγραμμα Ιράν

Πηγή: http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang

Τα σκουλήκια υπολογιστών, ένας από τους πιο κοινούς τύπους κακόβουλων λογισμικών, διασκορπίζονται στους υπολογιστές και τα δίκτυα τους, εκμεταλλευόμενα τις ευπάθειες των λειτουργικών τους συστημάτων. Ένα σκουλήκι υπολογιστή είναι ένα αυτόνομο πρόγραμμα που αυτοαντιγράφεται για να προσβάλλει άλλους υπολογιστές χωρίς να απαιτεί δράση από κανέναν. Επειδή διαμοιράζονται γρήγορα, συχνά χρησιμοποιούνται έτσι ώστε να εκτελέσουν ένα payload (φορτίο επί πληρωμή), δηλαδή ένα μέρος κώδικα που δημιουργήθηκε για να βλάψει ένα σύστημα. Τα payloads μπορούν επίσης να διαγράψουν αρχεία, να κρυπτογραφήσουν δεδομένα για μία επίθεση λυτρισμικού που θα δούμε στην επόμενη κυβερνοεπίθεση, να κλέψουν πληροφορίες και να φτιάξουν botnets (ζόμπι υπολογιστές που χρησιμοποιούνται για επιθέσεις άρνησης υπηρεσίας).[92]

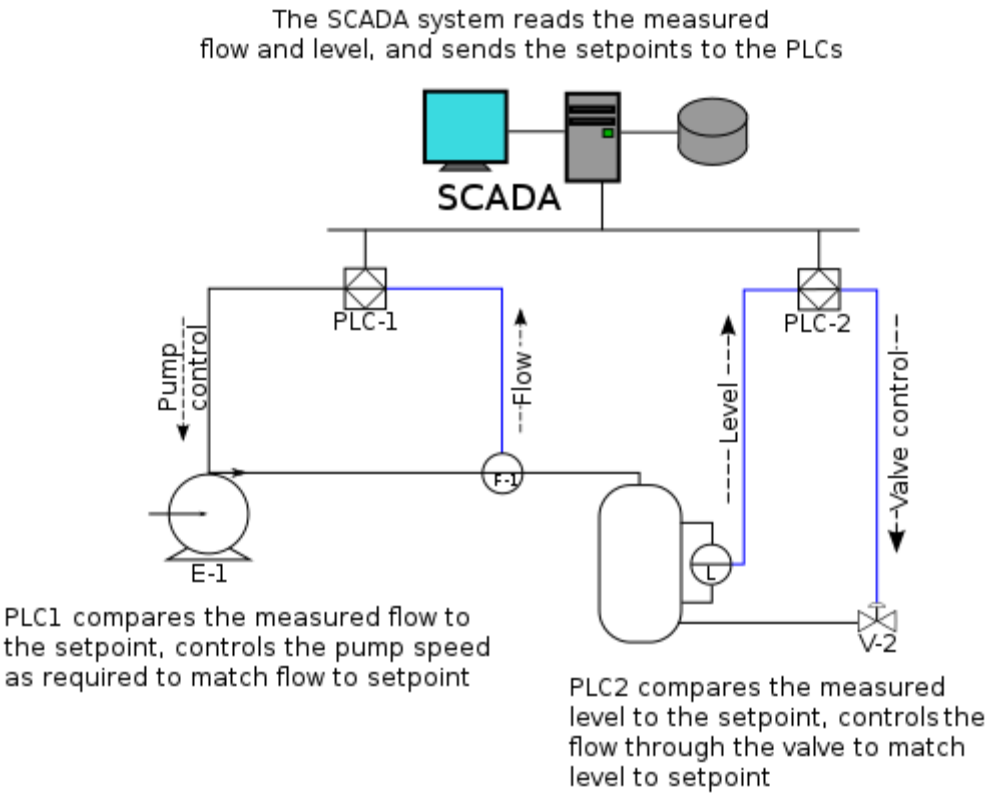
Εν προκειμένω, περί το 2010, το περίφημο σκουλήκι υπολογιστών Stuxnet, που φημολογείται ότι δημιουργήθηκε από τις μυστικές υπηρεσίες των Η.Π.Α. και του Ισραήλ, στοχοποίησε το σύστημα SCADA του πυρηνικού εργοστασίου του Ιράν, με κύριο σκοπό τον ολοκληρωτικό τερματισμό του Ιρανικού πυρηνικού προγράμματος.

Ο όρος SCADA (supervisory control and data acquisition) αναφέρεται σε μια κατηγορία συστημάτων ελέγχου και τηλεμετρίας βιομηχανικού αυτοματισμού. Τα συστήματα SCADA απαρτίζονται από τοπικούς ελεγκτές που ονομάζονται PLCs (Programmable Logic Controllers), οι οποίοι επιβλέπουν και διαχειρίζονται μεμονωμένα εξαρτήματα και μονάδες μιας εγκατάστασης. Αυτοί οι τοπικοί ελεγκτές συνδέονται με έναν κεντρικό σταθμό. Ο κεντρικός σταθμός εργασίας μπορεί στη συνέχεια να μοιραστεί τα δεδομένα που συλλέγει από την εγκατάσταση με πολλούς σταθμούς εργασίας σε ένα τοπικό δίκτυο LAN ή να μεταδώσει τα δεδομένα εγκατάστασης σε απομακρυσμένες τοποθεσίες χρησιμοποιώντας συστήματα τηλεπικοινωνιών, όπως ενσύρματα τηλεφωνικά δίκτυα ή ασύρματα δίκτυα.[93]

Δύναται επίσης κάθε τοπικός ελεγκτής να βρίσκεται σε απομακρυσμένη τοποθεσία και να μεταδίδει τα δεδομένα στον κεντρικό σταθμό είτε μέσω απλού καλωδίου, είτε ασύρματα χρησιμοποιώντας πομποδέκτη. Αυτή η διαμόρφωση περιλαμβάνει σταθερά μια ομάδα τοπικών ελεγκτών συνδεδεμένων σε μια τοπολογία αστέρα σε έναν κεντρικό σταθμό.[94]

[92] Πηγή: https://www.kaspersky.com/resource-center/threats/types-of-malware
[93] Πηγή: https://el.wikipedia.org/wiki/SCADA
[94] Πηγή: https://www.telstarinc.com/blog/how-scada-hmi-and-plc-work-together/

Εικόνα 58: Τοπικά PLCs συνδεδεμένα σε ένα κεντρικό masterstation



Πηγή: https://el.wikipedia.org/wiki/SCADA

Στις ικανότητες του Stuxnet λοιπόν, περιλαμβάνεται η παραποίηση των PLCs και ο έλεγχος των ηλεκτρομηχανολογικών διεργασιών των μηχανών, σε συσκευές με λειτουργικά συστήματα Windows. Πιο συγκεκριμένα, διείσδυσε στο σύστημα ελέγχου του πυρηνικού εργοστασίου παραγωγής ηλεκτρισμού του Ιράν και παραποίησε τη λειτουργία των προγραμματιζόμενων λογικών ελεγκτών που ήταν υπεύθυνοι για τους φυγοκεντρητές (μηχανήματα τα οποία χρησιμοποιούνται για τον εμπλουτισμό ουρανίου) και το διαχωρισμό των πυρηνικών υλικών, ενεργοποιώντας τους να στριφογυρνάνε σε ιλιγγιώδη ταχύτητα μέχρι να καταστραφεί όλος ο εξοπλισμός. Οπότε, το αποτύπωμα της κυβερνοεπίθεσης αυτής γρήγορα αποσταθεροποίησε τα πυρηνικά καύσιμα λόγω της αύξησης της περιστροφικής ταχύτητας του εξοπλισμού.

Το Stuxnet δε βλάπτει υπολογιστές αλλά όταν τους μολύνει, κάνει έναν έλεγχο για το αν αυτοί είναι συνδεδεμένοι με συγκεκριμένα μοντέλα Προγραμματιζόμενων Λογικών Ελεγκτών κατασκευασμένων από τη Siemens. Αξιοσημείωτο είναι πως εισχώρησε στην όλη υποδομή απλά μέσω ενός USB stick. Πιστεύεται ότι προσέβαλε πάνω από 20.000 υπολογιστές και κατέστρεψε τουλάχιστον το 1/5 των Ιρανικών φυγοκεντρητών, πηγαίνοντας το πυρηνικό πρόγραμμα χρόνια πίσω.

Προσοχή λοιπόν πρέπει να δοθεί πέρα από τους χρήστες οι οποίοι καλό θα ήταν να αποφεύγουν τα usb στικάκια σε υπολογιστές συνδεδεμένους με κρίσιμες υποδομές, και στους διαχειριστές των συστημάτων αυτών οι οποίοι καλό θα είναι να ορίζουν από την αρχή ποιοί υπολογιστές που είναι σε τι δίκτυο συνδεδεμένοι αν θα πρέπει να έχουν δικαιώματα ανάγνωσης / εγγραφής δεδομένων από εξωτερικές μονάδες αποθήκευσης.

3.13.3 WannaCry

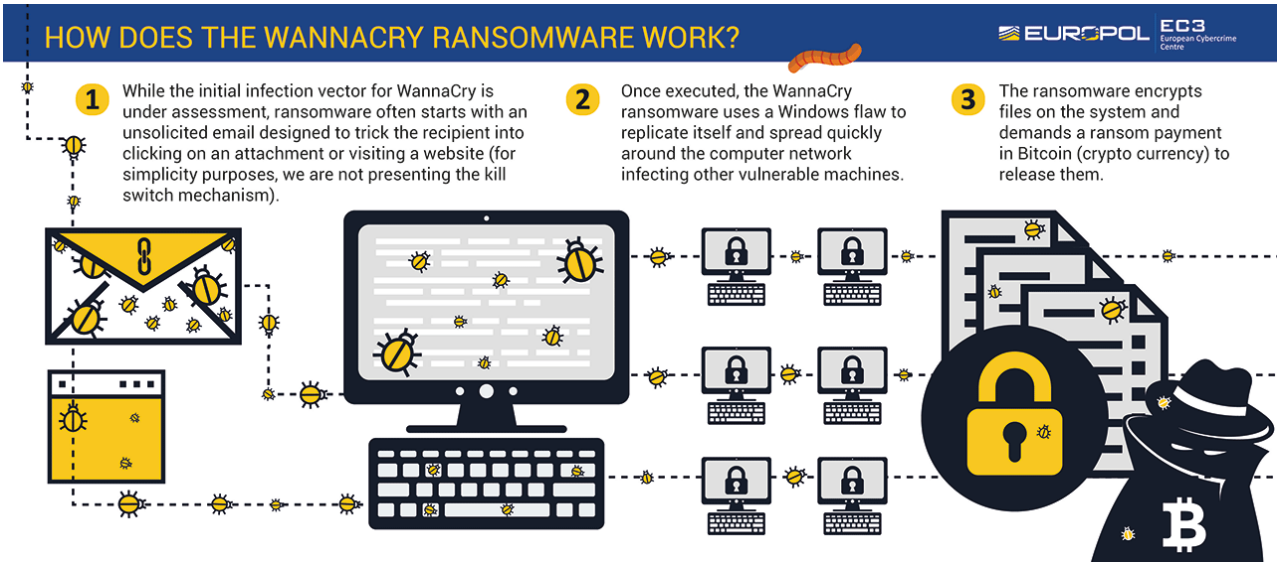
Είδος: Λυτρισμικό Κακόβουλο Σκουλήκι Υπολογιστών
(Ransomware Computer Malicious Worm)

Εικόνα59: WannaCry?

Πηγή: https://www.theverge.com/2017/6/14/15805346/wannacry-north-korea-linked-by-nsa

Το WannaCry είναι συνδυασμός σκουληκιού υπολογιστή και λυτρισμικού, δηλαδή εκτός από την ιδιότητα της ταχείας διάδοσης του σε ένα δίκτυο χωρίς εξωτερική παρέμβαση, κρυπτογραφεί τα δεδομένα αρχείων των χρηστών και τους ζητάει λύτρα σε bitcoin προκειμένου να αποκρυπτογραφηθούν στην κανονική μορφή τους. Πρωτοεμφανίστηκε και μεταδόθηκε ευρέως παγκόσμια στις 12 Μαΐου 2017 και εάν το ποσό των λύτρων δε πληρωνόταν στην ώρα του, τότε τα αρχεία σβήνονταν. Έχει μολύνει περισσότερους από 200.000 υπολογιστές επιχειρήσεων κι οργανισμών όπως τη Renault, την FedEx (πολυεθνική αμερικανική εταιρεία υπηρεσιών διαχείρισης αλυσίδας εφοδιασμού και αποστολής και παράδοσης) αλλά και απλούς μεμονωμένους χρήστες. Τη μεγαλύτερη ζημιά όμως την προκάλεσε στο αντίστοιχο Εθνικό Σύστημα Υγείας του Ηνωμένου Βασιλείου, το NHS (National Health Services). Οι υπολογιστές του NHS που μολύνθηκαν, οδήγησαν στην ακύρωση 19.000 ραντεβού και στην αναδρομολόγηση των ασθενοφόρων διακινδυνεύοντας πολλές ανθρώπινες ζωές. Πέραν αυτού, το συνολικό κόστος επιδιόρθωσης του IT συστήματος του NHS κόστισε 92.000.000 λίρες για τον καθαρισμό της απειλής και την αναβάθμιση του.

Εικόνα 60: Λειτουργία WannaCry



Πηγή: https://www.europol.europa.eu/wannacry-ransomware

Σύμφωνα με το Ευρωπαϊκό Κέντρο Κυβερνοεγκλήματος (European Cybercrime Centre - EC3) της Europol, το WannaCry εκμεταλλεύεται την ευπάθεια MS17-010 στην εφαρμογή του Microsoft Protocol Server Block Protocol (SMB). Το SMB είναι ένα πρωτόκολλο των λειτουργικών συστημάτων Windows για διαμοιρασμό αρχείων σε τοπικά δίκτυα υπολογιστών. Μπορεί να δουλεύει ακόμα σε παλαιότερες εκδόσεις των Windows που δεν υποστηρίζονται πια όπως τα Windows XP, 8, Vista και Windows Server 2003.

3.13.3.1 Προστασία έναντι WannaCry

Η αποκρυπτογράφηση των κρυπτογραφημένων WannaCry αρχείων δεν είναι δυνατή επί του παρόντος. Γι' αυτό συστήνεται προληπτικά:

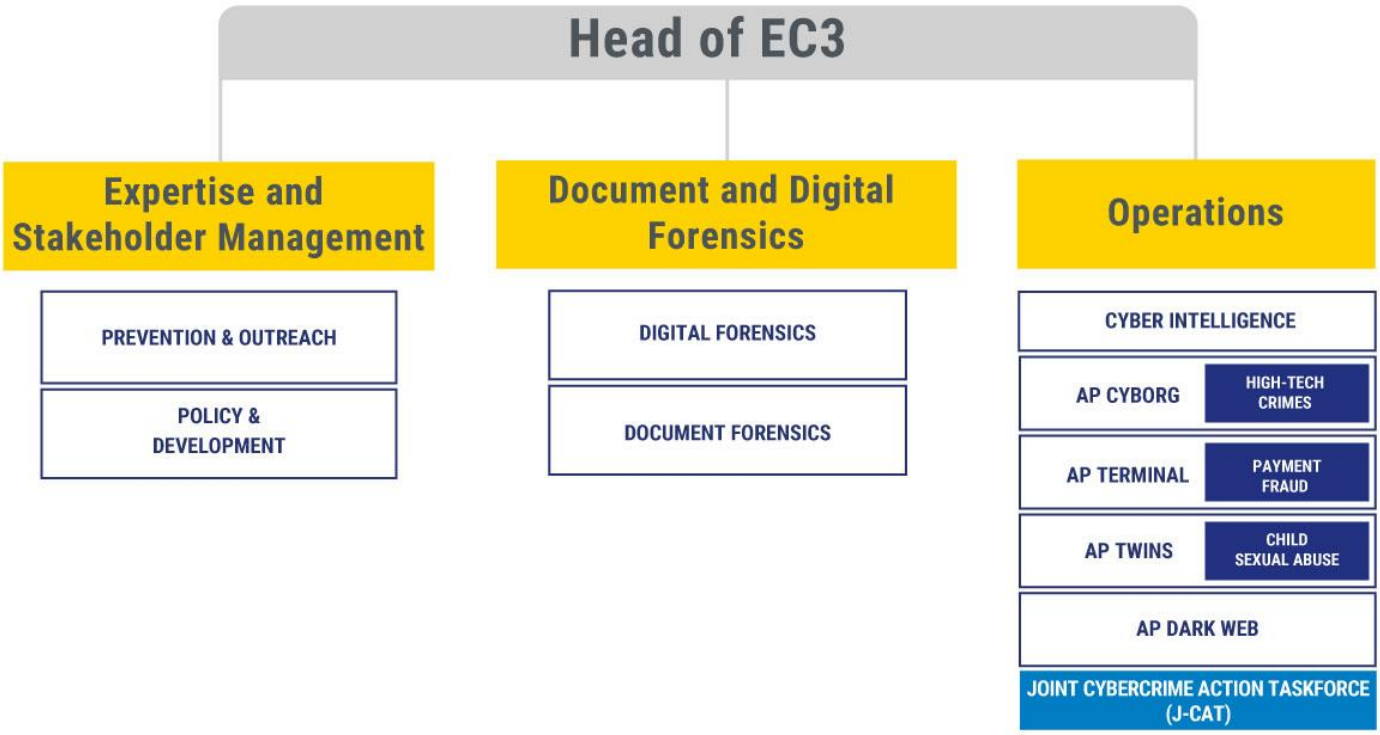
1) Να λαμβάνονται backups ανά τακτά χρονικά διαστήματα στο σύστημα και στα αρχεία του.
2) Η δημιουργία σημείων επαναφοράς (Restore Points) στα παλαιότερα Client λειτουργικά συστήματα Windows κι αντίστοιχα σωστή ρύθμιση του Volume Shadow Copies στα Windows Server.
3) Χρήση αντιικού προγράμματος προστασίας υπολογιστή, ενημερωμένο με τις τελευταίες υπογραφές των τελευταίων ιών που κυκλοφορούν.
4) Απενεργοποίηση του SMB πρωτοκόλλου ακολουθώντας τις οδηγίες: https://docs.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3
5) Στις συσκευές δικτύου, κλείσιμο των θυρών των πρωτοκόλλων επικοινωνίας (UDP, TCP) που χρησιμοποιεί το SMB πρωτόκολλο για τη λειτουργία του, ενδεικτικά στην πρώτη του έκδοση SMBv1, τις θύρες 137, 138 στο UDP και 139, 445 στο TCP.
6) Ενεργοποίηση της εμφάνισης της κατάληξης των αρχείων στο λειτουργικό σύστημα Windows (Show file extensions), που καθιστά τον εντοπισμό πιθανά βλαβερών αρχείων ευκολότερο. Εάν π.χ. λάβουμε ένα συνημμένο αρχείο με κατάληξη '.exe', '.com', '.vbs' ή '.scr' προφανώς δεν πρέπει να το ανοίξουμε. Συνήθης τακτική των κυβερνοεγκληματιών η μεταμφίεση

κανονικών αρχείων όπως hot-chics.avi.exe ή report.doc.scr. Εάν λοιπόν δεν είναι ενεργοποιημένη αυτή η λειτουργία, θα δούμε το report.doc και νομίζοντας πως είναι .doc θα τρέξει το .scr κακόβουλο αρχείο.

7) Τοποθέτηση κανόνα στο αντιικό προστασίας ή στο firewall που θα αποτρέπει τη δημιουργία .wnry αρχείων.

Τέλος, συστήνεται σε κάθε περίπτωση να μην πληρωθούν ποτέ λύτρα, καθώς πέραν του ότι δεν πρέπει να υποστηρίζονται δραστηριότητες κυβερνοεγκληματιών, δεν υπάρχει εγγύηση ότι το πρόβλημα θα λυθεί.

Εικόνα 61: Οργανόγραμμα του Ευρωπαϊκού Κέντρου Κυβερνοεγκλήματος



Πηγή: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

3.14 Πολιτική Ασφαλείας για ισχυρούς κωδικούς

Ο καλύτερος συνδυασμός μνημόνευσης και πολυπλοκότητας, ώστε να μη μαντεύεται από τους επιτιθέμενους, με τη σημερινή διαθέσιμη τεχνολογία, είναι να έχουμε μία περίεργη φράση συνδυασμένη με σύμβολα αντί για κενά μεταξύ των λέξεων.

Έστω ότι έχουμε έναν κωδικό της μορφής: fkJl096%$hsj387

Ο παραπάνω κωδικός δεν είναι και ο καλύτερος που μπορεί να υπάρξει, παρότι συνίστανται συχνά φράσεις που δε βγάζουν νόημα ώστε να μειώνονται οι πιθανότητες να σπάσουν από αλγορίθμους λεξικών σε bruteforce επιθέσεις, κυρίως γιατί δεν είναι ευμνημόνευτος.

Το πλήθος των χαρακτήρων (ας πούμε Π) είναι 15 δεν είναι ούτε μεγάλο ούτε μικρό, ενώ το εύρος κάθε χαρακτήρα σε ένα τυπικό πληκτρολόγιο (characterset) είναι το εξής[95]:

Numbers (0-9): 10

Lower Case Latin Alphabet (a-z): 26

Lower Case & Upper Case Latin Alphabet (a-z, A-Z): 52

ASCII Printable Character Set (a-z, A-Z, symbols, space): 95

Άρα, ο αριθμός των πιθανών συνδυασμών είναι ο 95^{15}

Η εντροπία του είναι $\log_2(9515)$.

Σίγουρα θα σπάσει δύσκολα με τα τωρινά δεδομένα, αλλά όπως προείπαμε είναι δυσμνημόνευτος. Συνεπώς θα προτιμήσουμε passphrases με δικούς μου μνημονικούς κανόνες. Λέξεις που βγάζουν νόημα με περισσότερο (διπλάσιο, τριπλάσιο από όσο θα βάζαμε) πλήθος χαρακτήρων και με συνδυασμό συμβόλων ευμνημόνευτων όπως αντικατάσταση κενών στις μεταξύ φράσεις με το σύμβολο %. Μία περίεργη φράση του στυλ:

Poios%Fylaei%Tous%Fylakes%Mas%Oeo

3.15 Προτεινόμενα Μέτρα Ασφαλείας Έξυπνων Δικτύων

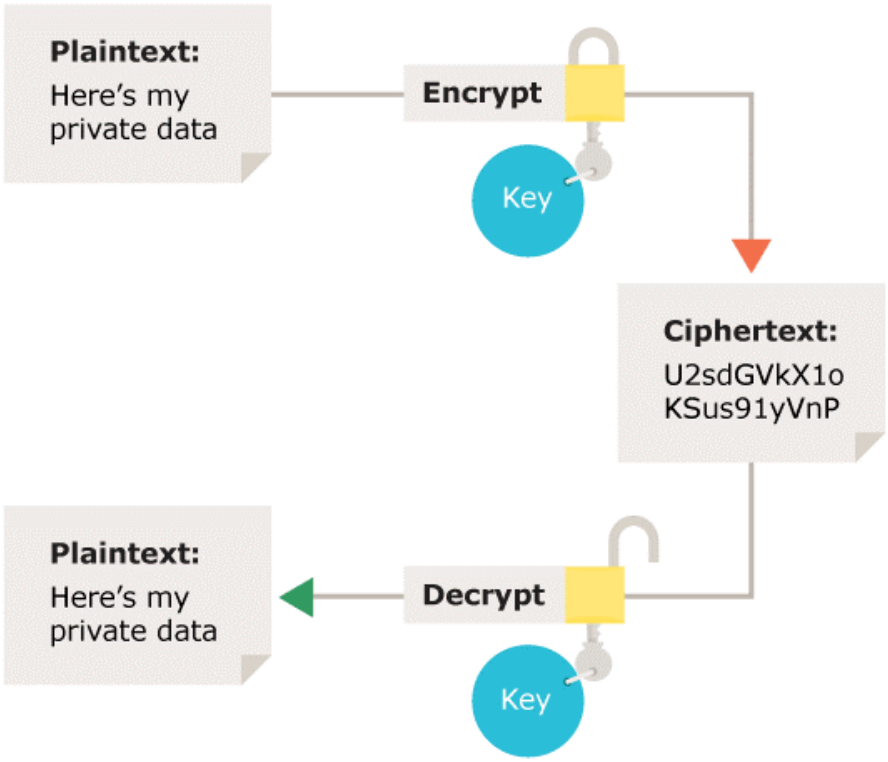
Είδαμε αρκετούς τρόπους προστασίας έναντι των προηγούμενων κυβερνοεπιθέσεων. Η καλύτερη μέθοδος αντιμετώπισης κινδύνων και ρίσκων όσον αφορά τα δίκτυα και τα συστήματα όμως είναι η πρόληψη. Η υιοθέτηση των παρακάτω αρχών κρίνεται απαραίτητη για το σχεδιασμό ολοκληρωμένων λύσεων ασφαλείας για τα έξυπνα δίκτυα παροχής ηλεκτρικού ρεύματος.

[95] Πηγή: https://generatepasswords.org/how-to-calculate-entropy/

3.15.1 Κρυπτογράφηση

Η κρυπτογράφηση είναι η διαδικασία της κωδικοποίησης των δεδομένων, πληροφοριών, μηνυμάτων που αποστέλλονται σε ένα δίκτυο, από τον αποστολέα στον παραλήπτη, έτσι ώστε να μην είναι αναγνώσιμα από όλους τους ενδιάμεσους κόμβους, αλλά να είναι αναγνώσιμα μόνο από τον τελικό παραλήπτη. Σήμερα, δύο κύριοι ευρέως διαδεδομένοι τύποι κρυπτογράφησης είναι οι Συμμετρικοί και οι Ασύμμετροι. Η συμμετρία ή όχι αφορά το κλειδί κρυπτογράφησης κι αποκρυπτογράφησης των δεδομένων αν είναι το ίδιο ή όχι.

Εικόνα 62: Συμμετρική Κρυπτογράφηση – Ίδιο κλειδί κρυπτογράφησης κι αποκρυπτογράφησης



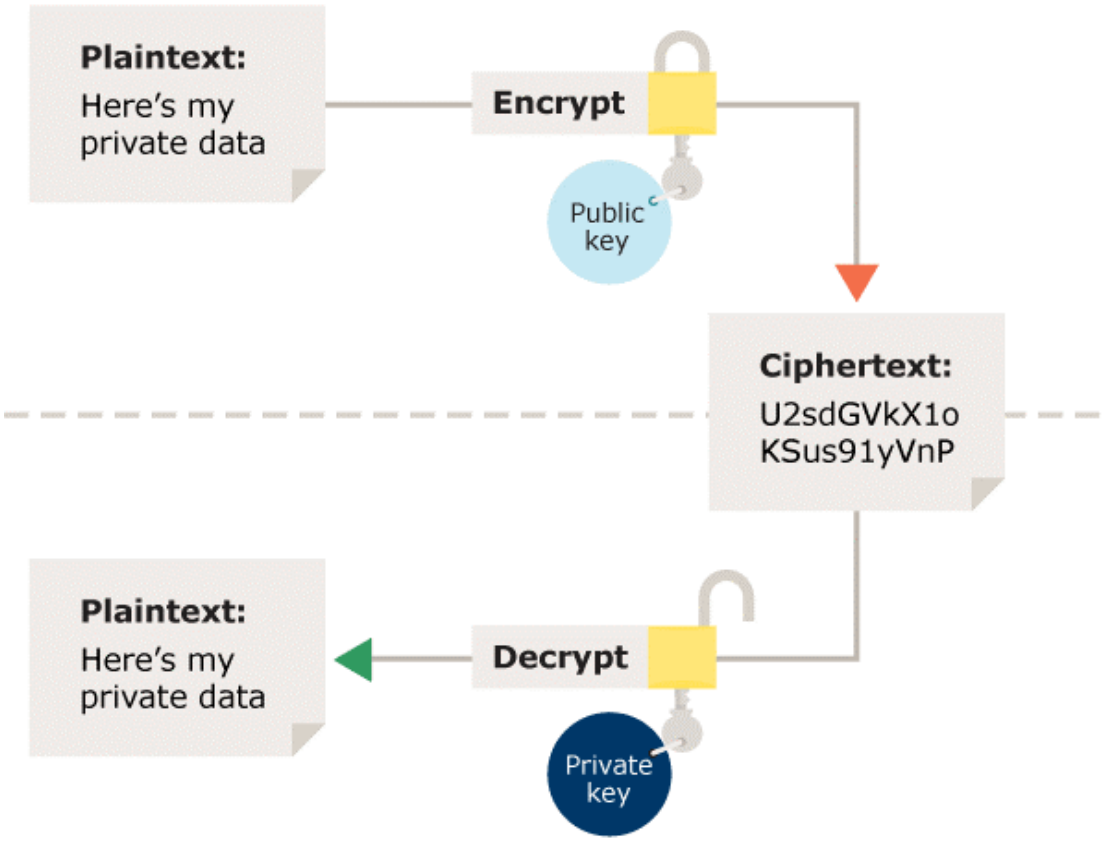
Πηγή: https://ico.org.uk/media/images/other/2260256/symmetric.gif

Στη Συμμετρική κρυπτογράφηση πρέπει ωστόσο να διασφαλιστεί πλήρως το κανάλι μετάδοσης κλειδιού από τον αποστολέα στον παραλήπτη.

Στην Ασύμμετρη κρυπτογράφηση κάθε χρήστης διαθέτει ένα Δημόσιο κι ένα Ιδιωτικό κλειδί. Πάντα το Δημόσιο δύναται να είναι διαθέσιμο οπουδήποτε ενώ το Ιδιωτικό το γνωρίζει μόνο αυτός. Η φιλοσοφία εδώ είναι η εξής: ο αποστολέας χρησιμοποιεί το Δημόσιο κλειδί του παραλήπτη προκειμένου να κρυπτογραφήσει το μήνυμα, κι ο παραλήπτης είναι σε θέση να αποκρυπτογραφήσει το μήνυμα μόνο με το Ιδιωτικό του κλειδί.[96]

[96] Πηγή: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-types-of-encryption-are-there/

Εικόνα 63: Ασύμμετρη Κρυπτογράφηση – Χρήση διαφορετικών κλειδιών για Κρυπτογράφηση κι Αποκρυπτογράφηση



Πηγή: https://ico.org.uk/media/images/other/2260261/asymmetric.gif

Σήμερα, χρησιμοποιείται και συστήνεται η κρυπτογράφηση AES (Advanced Encryption Standard) 256-bit από τους πιο γνωστούς παρόχους υπηρεσιών VPN. Τα 256 bits είναι το πλήθος των ψηφίων του κλειδιού κρυπτογράφησης, πρόκειται για αρκετά μεγάλο εύρος πιθανών συνδυασμών, περισσότερο κι από τα αστέρια του σύμπαντος. Γι' αυτό το λόγο χρησιμοποιείται από κυβερνήσεις και τράπεζες παγκόσμια, για τη διασφάλιση των δεδομένων τους.

3.15.2 Αυθεντικοποίηση

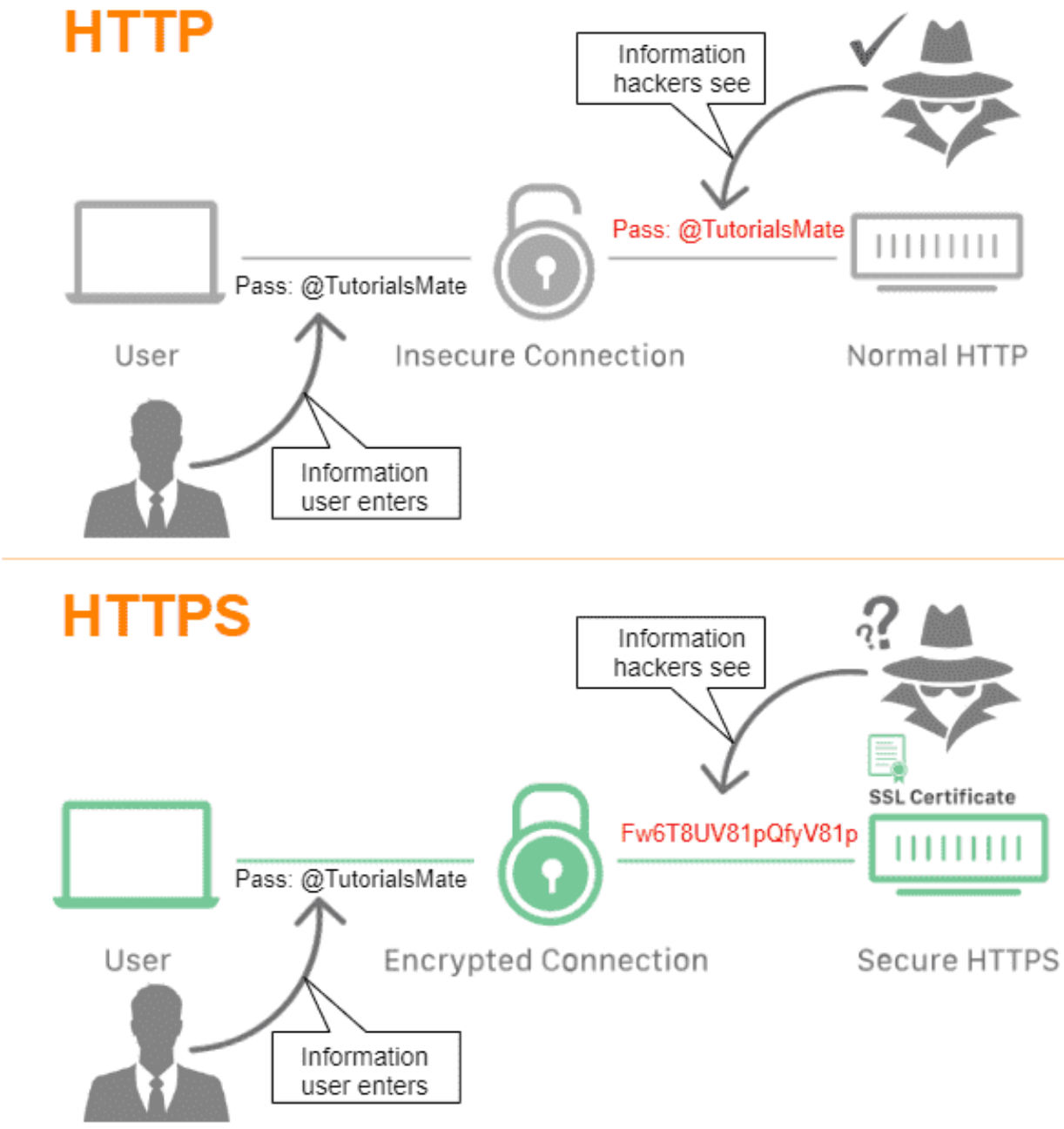
Η διατήρηση της αυθεντικοποίησης και του ελέγχου πρόσβασης σε όλες τις εφαρμογές και υποδομές των έξυπνων δικτύων παροχής ηλεκτρικού ρεύματος πρέπει διαρκώς να ελέγχεται από τους ειδικούς (IT και χειριστές συστημάτων ελέγχου) προκειμένου να εξασφαλίζεται η ομαλή λειτουργία τους. Ισχυροί μηχανισμοί αυθεντικοποίησης σημαίνει ότι έχουν οριστεί και απονεμηθεί όλα τα εμπλεκόμενα είδη χρηστών των πληροφοριακών συστημάτων με τα αντίστοιχα δικαιώματα τους. Με αυτόν τον τρόπο ο διαχειριστής μπορεί να έχει πρόσβαση σε όλες τις δράσεις των χρηστών και συγκεκριμένοι χρήστες να έχουν τις κατάλληλες προσβάσεις με περιορισμένη εξουσιοδότηση στο τι μπορούν να κάνουν και με περιορισμένη πρόσβαση σε δεδομένα που αφορούν μόνο τις εργασίες τους. Αυτό μειώνει και τον κίνδυνο έκθεσης πολύτιμων δεδομένων σε περίπτωση που χακαριστεί οποιοσδήποτε με περιορισμένη πρόσβαση. Επιτυγχάνεται επίσης η ιχνηλασιμότητα, δηλαδή η

ακριβής ανάλυση του πότε έγινε τι από ποιόν στο δίκτυο ή στις εργασίες των έξυπνων δικτύων. Η αυθεντικοποίηση μπορεί να επιτευχθεί με τη χρήση των κρυπτογραφικών προτοκόλλων SSL (Secured Socket Layer) και Transport Layer Security (TLS) που χρησιμοποιούνται ευρέως κατά τη μεταφορά δεδομένων μεταξύ των εξυπηρετητών, των πληροφοριακών συστημάτων, των ηλεκτρονικών εφαρμογών και των χρηστών.

Εικόνα 64: Αυθεντικοποίηση και Εξουσιοδότηση

Πηγή: https://medium.com/geekculture/authentication-and-authorization-a5a2eafdde16

Εικόνα 65: HTTP vs HTTPS – Χρήση πρωτοκόλλου SSL κατά την πρόσβαση σε ιστοσελίδες

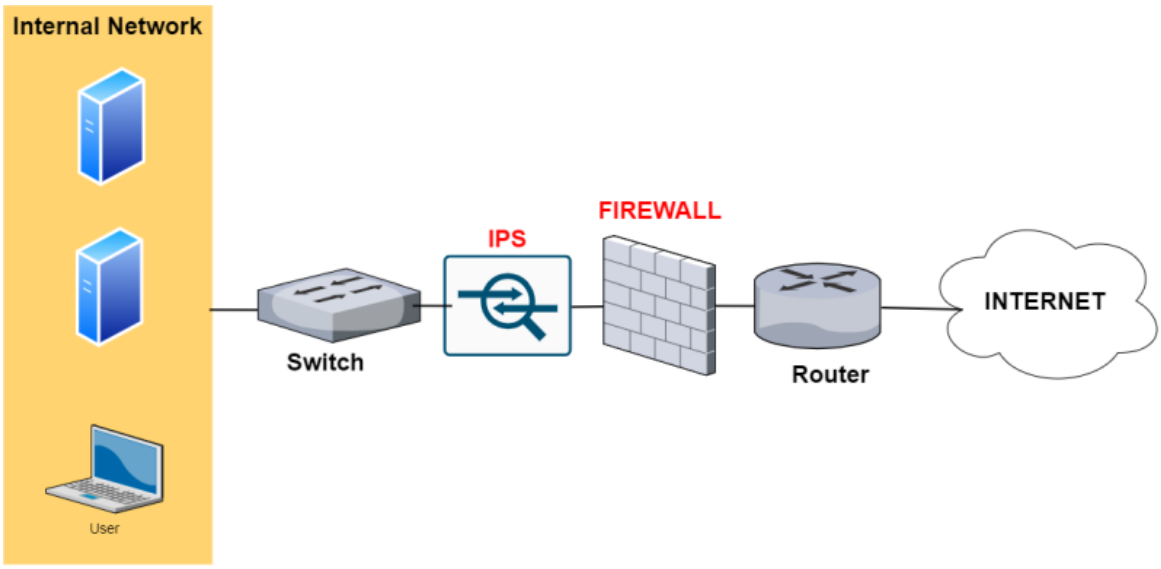


Πηγή: https://www.tutorialsmate.com/2020/07/http-vs-https.html

3.15.3 Προστασία Απειλών με Αντιικά, IPS και IDS

Για όλα τα πληροφοριακά συστήματα που είναι συνδεδεμένα στο έξυπνο δίκτυο παροχής ηλεκτρικής ενέργειας κρίνεται αναγκαίο πως πρέπει να έχουν αντιικά προστασίας διαρκώς ενημερωμένα. Επιπλέον η χρήση Συστημάτων Αποτροπής Εισδοχής (Intrusion Prevention System / IPS), για τον έλεγχο κίνησης, επιθέσεων και ευπαθειών σε ένα δίκτυο μπορεί να αποτρέψει συγκεκριμένες κυβερνοεπιθέσεις. Αυτά τα συστήματα έχουν σχεδιαστεί ώστε να επιτηρούν δεδομένα που αφορούν εισδοχή στο δίκτυο και να λαμβάνουν άμεση δράση ώστε να αποτραπεί η ανάπτυξη μίας κυβερνοεπίθεσης. Λειτουργούν συγκρίνοντας την κίνηση με υπογραφές ήδη γνωστών απειλών που υπάρχουν στη βάση δεδομένων τους. Εάν εντοπίσουν στην κίνηση κάποιο πακέτο με την υπογραφή γνωστής απειλής τότε άμεσα διακόπτεται και μπλοκάρεται η κίνηση των δεδομένων. Δύναται επίσης να δουλέψει με ανίχνευση μη συνηθισμένης διακίνησης των δεδομένων βασιζόμενη σε στατιστικές προηγουμένων διακινήσεων, σύμφωνα με κανόνες που έχουν οριστεί σε αυτό από το διαχειριστή του συστήματος.

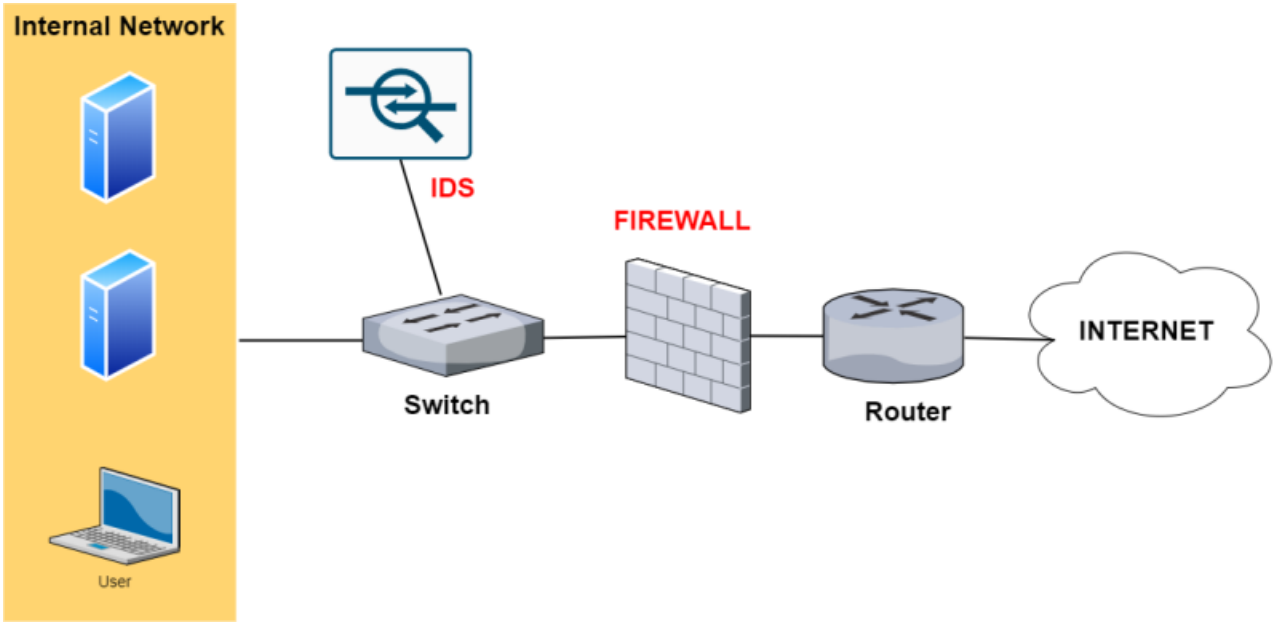
Εικόνα 66: Διάγραμμα μίας υποδομής με IPS



Πηγή: https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867?page=2

Πέραν αυτών, υπάρχουν και τα Συστήματα Ανίχνευσης Εισδοχής (Intrusion Detection System / IDS) τα οποία χρησιμοποιούνται για να επιτηρήσουν και να αναλύσουν την κίνηση των δεδομένων στα δίκτυα επικοινωνίας, τα οποία προστατεύουν το σύστημα από απειλές που προέρχονται από το διαδίκτυο. Πρόκειται για τον προκάτοχο των IPS εφόσον αυτά όπως θα δούμε στην παρακάτω εικόνα, τα δεδομένα περνάνε παράλληλα και σε αυτά και στο εσωτερικό δίκτυο άρα δεν είναι σε θέση να κόψουν την κίνηση κι απλά προειδοποιούν παθητικά ότι κάτι δεν πάει καλά στο δίκτυο.

Εικόνα 67: Διάγραμμα μίας υποδομής με IDS

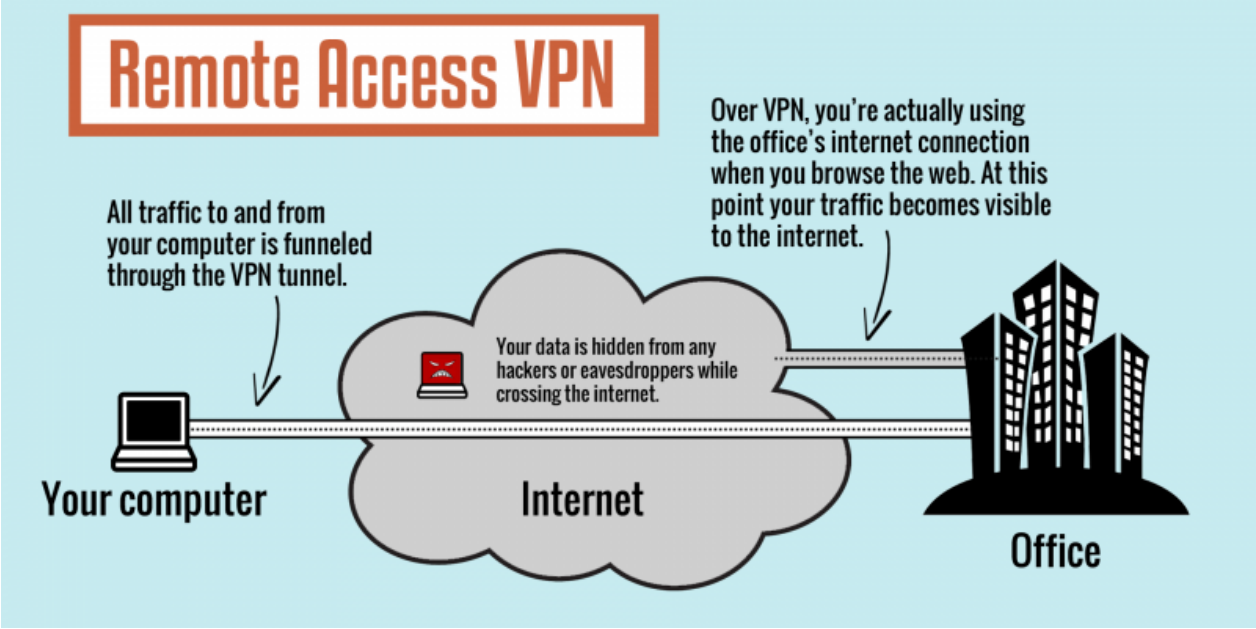


Πηγή: https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867?page=2

3.15.4 Χρήση Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network)

Το Εικονικό Ιδιωτικό Δίκτυο (VPN) παρέχει επιπλέον ασφάλεια όταν απαιτείται χρήση δημοσίου δικτύου, όπως δηλαδή η χρήση του Διαδικτύου. Τα VPN χρησιμοποιούν ποικιλία διαφόρων μεθόδων ασφαλείας, όπως την κρυπτογραφημένη επικοινωνία και προστασία δεδομένων που μεταφέρονται σε όλη την υποδομή των έξυπνων δικτύων. Οι δύο επικρατέστεροι κύριοι τύποι αυτής της τεχνολογίας, είναι οι Απομακρυμένης Πρόσβασης VPN (Remote Access VPN) και Site To Site VPN.

Εικόνα 68: Remote Access VPN Παράδειγμα Επικοινωνίας Χρήστη με Οργανισμό εργασίας του

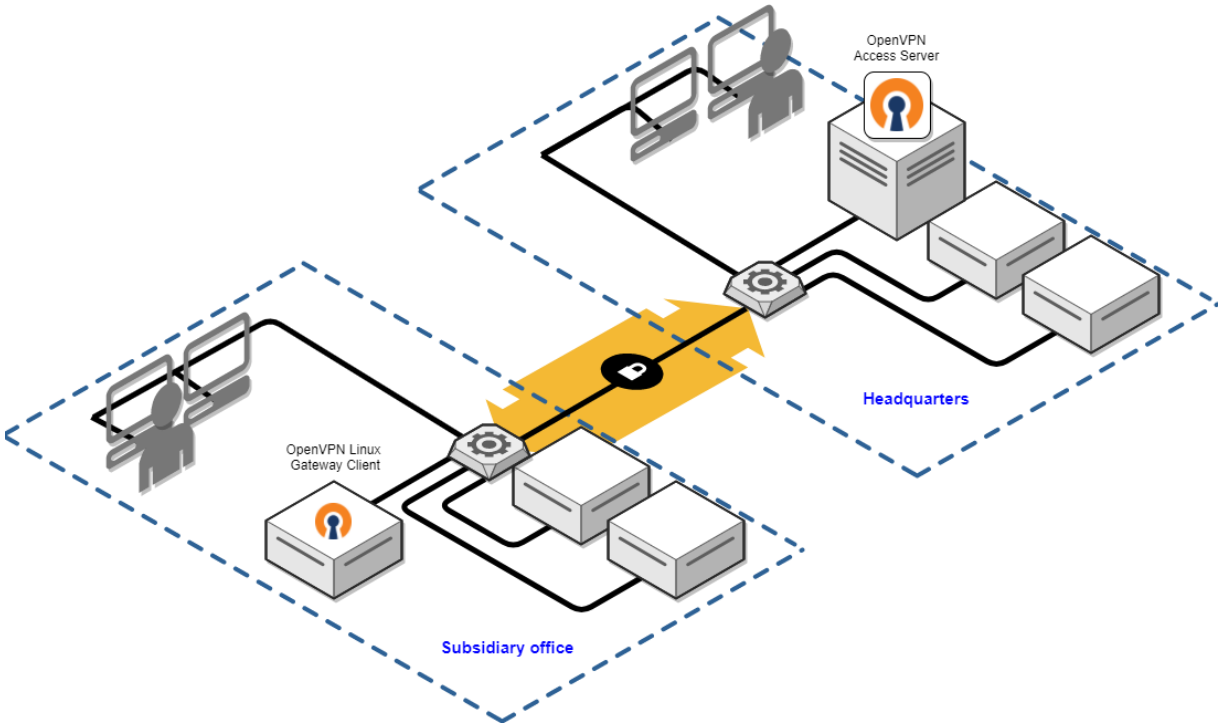


Πηγή: https://cbm.com.au/remote-access-vpn-security/cbm-corporate-remote-access-vpn/

Το Remote Access VPN χρησιμοποιεί το Διαδίκτυο ώστε να επικοινωνήσει ο χρήστης με τον οργανισμό του και να αποκτήσει πρόσβαση στο ιδιωτικό δίκτυο του. Η αυθεντικοποίηση του χρήστη γίνεται από τον οργανισμό και αφού ταυτοποιηθεί έγκυρα ο χρήστης αποκτά πρόσβαση σε όλους τους πόρους του (αρχεία, έγγραφα) σα να είναι στην εταιρεία. Ενδείκνυται συνεπώς για τηλεεργασία ή ακόμα και για απομακρυσμένη πρόσβαση για επίλυση προβλημάτων.

Το Site To Site VPN δουλεύει παρόμοια, απλά για μεγαλύτερης κλίμακας συνδέσεις καθώς διασυνδέει ολόκληρα δίκτυα παραρτημάτων διαφόρων τοποθεσιών με τη κεντρική υποδομή του οργανισμού. Χρησιμοποιείται συνεπώς από μεγάλους οργανισμούς, οπότε κρίνεται αναγκαίο για τη διασύνδεση των περιφερειακών μονάδων των έξυπνων δικτύων παροχής ηλεκτρικού ρεύματος και την ομαλή λειτουργία όλου του οργανισμού τους.

Εικόνα 69: Site To Site VPN Παράδειγμα Επικοινωνίας Κεντρικής Υποδομής με Παράρτημα



Πηγή: https://openvpn.net/vpn-server-resources/site-to-site-routing-explained-in-detail/

3.16 Συμπεράσματα 3ου Κεφαλαίου

Η επόμενη γενιά του ηλεκτρικού δικτύου, ήτοι τα Έξυπνα Δίκτυα, αναμένεται να εφαρμοστεί στο εγγύς μέλλον λόγω των πολυάριθμων πλεονεκτημάτων του, όπως την αυξημένη ευελιξία, την αποδοτικότητα και το μειωμένο κόστος λειτουργίας τους. Επιπλέον, η ενσωμάτωση σύγχρονων τεχνολογιών επικοινωνίας και καινοτόμων εφαρμογών Τεχνητής Νοημοσύνης αναμένεται να επιταχύνει την αναβάθμιση του παραδοσιακού δικτύου.

Σε αυτό το κεφάλαιο, διεξήχθη μια επισκόπηση των Έξυπνων Δικτύων με βάση την αρχική και σύγχρονη έρευνα, η οποία εξετάζει τα δομικά ζητήματα αυτών των δικτύων. Είναι αξιοσημείωτο ότι τα παραδοσιακά δίκτυα που χρησιμοποιούνται αυτή τη στιγμή είναι αρκετά παλιά εφόσον υφίστανται ήδη έναν αιώνα. Δεδομένης της εξέλιξης της τεχνολογίας και των αυξανόμενων ενεργειακών αναγκών, έχει καταστεί απαραίτητη η μετάβαση από το υπάρχον δίκτυο σε αυτό που είναι γνωστό ως Ευφυές Δίκτυο. Ένα χαρακτηριστικό γνώρισμα του Έξυπνου Δικτύου είναι η αμφίδρομη σχέση επικοινωνίας μεταξύ παραγωγής και κατανάλωσης ενέργειας. Αυτό έρχεται σε αντίθεση με το παραδοσιακό δίκτυο, όπου η ροή είναι μόνο προς μία κατεύθυνση, από την παραγωγή στην κατανάλωση. Η επιτυχία του Smart Grid εξαρτάται όχι μόνο από την υποδομή, συμπεριλαμβανομένων των συσκευών και του λογισμικού, αλλά και από την ικανότητά του να παρέχει καθολικά υπηρεσίες και να ανταποκρίνεται σε διάφορες ανάγκες. Η εφαρμογή του Smart Grid απαιτεί λύσεις και πρακτικές που υπερβαίνουν τις δυνατότητες του σημερινού δικτύου. Με την ενσωμάτωση των αναπτυσσόμενων τεχνολογιών επικοινωνίας, μετάδοσης και αποθήκευσης, μπορούμε να προσφέρουμε πιο σταθερές, αξιόπιστες και ασφαλέστερες υπηρεσίες με ταχύτερους χρόνους διεκπεραίωσης. Η μετάβαση στο Έξυπνο Δίκτυο στοχεύει να είναι πιο οικονομική από πλευράς ενέργειας, ενώ φέρνει επίσης σημαντικά περιβαλλοντικά οφέλη στις πόλεις και εν γένει στον πλανήτη που κατοικούμε.

Κάθε κόμβος διασύνδεσης δικτύου χρησιμεύει ως ένα μικρό κύτταρο που συμβάλλει στη λειτουργία του Έξυπνου Δικτύου. Στην πραγματικότητα, κάθε έξυπνη συσκευή παίζει καθοριστικό ρόλο σε αυτό το εκτεταμένο δίκτυο που διευκολύνει τη μεταφορά ενέργειας και πληροφοριών. Λαμβάνοντας υπόψη τα πιθανά πλεονεκτήματα, μια έξυπνη πόλη θα μπορούσε να λειτουργήσει ως πλατφόρμα για την παρακολούθηση της συμπεριφοράς και των πλεονεκτημάτων του Έξυπνου Δικτύου. Συγκεκριμένα, οι εφαρμογές που αναπτύχθηκαν για το σκοπό αυτό περιλαμβάνουν διάφορες πτυχές της ζωής στην πόλη και ορισμένες από αυτές έχουν ήδη εφαρμοστεί σε πόλεις σε όλη την Ευρώπη και τον κόσμο.

Μια σημαντική πτυχή των έξυπνων δικτύων είναι η παρουσία έξυπνων μετρητών. Αυτοί οι μετρητές, μαζί με τα συστήματα οικιακής διαχείρισης ενέργειας, επιτρέπουν στους καταναλωτές να διαχειρίζονται αποτελεσματικά τη χρήση ενέργειας παρέχοντας ανατροφοδότηση σχετικά με τη ζήτηση και τους ρυθμούς κατανάλωσης της ενέργειας. Ενθαρρύνουν τους καταναλωτές να χρησιμοποιούν ενέργεια σε περιόδους χαμηλής ζήτησης ώστε να επιτύχουν πιο οικονομική κατανάλωση, συμβάλλοντας έτσι στη μείωση της συμφόρησης του δικτύου. Επιπλέον, μέσω της χρήσης έξυπνων συσκευών, οι καταναλωτές θα δύνανται να λαμβάνουν ειδοποιήσεις όταν τα επίπεδα ζήτησης υπερβούν ένα συγκεκριμένο όριο, ωθώντας τους να απενεργοποιήσουν τις περιττές συσκευές μέχρι να μειωθεί η ζήτηση, είτε βρίσκονται στην οικεία είτε εκτός.

Σύμφωνα με την πολιτική της Ε.Ε. που κατέστησε αναγκαία την εφαρμογή των Έξυπνων Δικτύων, η Ευρωπαϊκή Ένωση παραμένει αφοσιωμένη στην επίτευξη των στόχων 20-20-20. Δηλαδή, μέχρι το έτος 2020, η ΕΕ στόχευσε να μειώσει τις εκπομπές αερίων θερμοκηπίου κατά 20% σε σύγκριση με τα επίπεδα του 1990, να παράγει το 20% της ενέργειας από ανανεώσιμες πηγές, με αποτέλεσμα τη μείωση της κατανάλωσης ενέργειας κατά 20% και να αντικαταστήσει επιτυχώς το 80% των μετρητών με έξυπνους μετρητές. Αξίζει να σημειωθεί ότι το σχέδιο αυτό ήταν σε μεγάλο βαθμό επιτυχημένο.

Εκτός από τη σημασία της προστασίας του περιβάλλοντος, είναι ευρέως αποδεκτό ότι οι τρέχουσες δραστηριότητές μας εξαρτώνται σε μεγάλο βαθμό από την ηλεκτρική ενέργεια, αναδεικνύοντας την ανάγκη ενός αξιόπιστου και σταθερού δίκτυου ζωτικής σημασίας. Η εμφάνιση διακοπών στο δίκτυο ηλεκτρικής ενέργειας επηρεάζει σε μεγάλο βαθμό τόσο τις κυβερνήσεις όσο και τις επιχειρήσεις. Υπό το πρίσμα αυτό, και τα κράτη και η Ευρωπαϊκή Ένωση αναγνωρίζουν την αναγκαιότητα αναβάθμισης του υφιστάμενου ηλεκτρικού δικτύου και διαθέτουν κονδύλια για την έρευνα και ανάπτυξη Έξυπνων Δικτύων για τα κράτη μέλη.

Μετά την παρατήρηση των εφαρμογών των Έξυπνων Δικτύων στην Ευρώπη και παγκοσμίως, είναι προφανές ότι στο μέλλον η τεχνολογία τους θα περιστρέφεται γύρω από το συνδυασμό υφιστάμενων και αναπτυσσόμενων τεχνολογιών, με εξέχοντα ρόλο της Τεχνητής Νοημοσύνης στη λήψη αποφάσεων. Ορισμένες χώρες της Ευρωπαϊκής Ένωσης πραγματοποιούν ήδη εκτεταμένες δοκιμές σχετικά με την έξυπνη μέτρηση και την αποθήκευση της ενέργειας. Ωστόσο, είναι σημαντικό να θυμόμαστε ότι εν μέσω της ζήτησης για νέες τεχνολογίες και καινοτομιών, η εστίαση πρέπει πάντα να είναι στην ευημερία των ατόμων. Η ιεράρχηση του αντίκτυπου στην καθημερινή ζωή των ανθρώπων και η ικανότητα επίλυσης πραγματικών προβλημάτων, αντί της δημιουργίας τεχνολογίας μόνο για χάρη του κέρδους, θα πρέπει να καθοδηγεί τις διαδικασίες λήψης αποφάσεων.

Επιπλέον, είναι σημαντικό να αντιμετωπιστεί το ζήτημα της ανάπτυξης τεχνολογίας τόσο για την ενδοδικτυακή επικοινωνία όσο και για την ασφάλεια των μεταδιδόμενων δεδομένων και του εξοπλισμού των δικτύων παροχής ηλεκτρικού ρεύματος. Οι πιθανές απώλειες θα μπορούσαν να είναι σημαντικές, γεγονός που υπογραμμίζει την ανάγκη για τη δημιουργία ισχυρών πρωτοκόλλων και αλγορίθμων.

Σχεδόν όλες οι έρευνες ανέδειξαν πως η πιο καταστροφική απειλή που αφορά τα Έξυπνα Δίκτυα παροχής ηλεκτρικής ενέργειας είναι η άρνηση της υπηρεσίας. Προσβάλλοντας το δίκτυο τους θα κατέρρεε όλη η λειτουργία τους, που είναι και η πιο σημαντική, η παροχή του ηλεκτρικού ρεύματος, όπως έγινε με το κακόβουλο λογισμικό Trojan Horse Black Energy στην Ουκρανία. Γι’ αυτό απαιτείται μία καθολική προσέγγιση ασφαλείας σε όλα τα επίπεδα, από την υιοθέτηση κουλτούρας ασφαλείας (χρήση ισχυρών κωδικών, αποφυγή phishing) από τον υπάλληλο που δουλεύει σε έναν τέτοιο οργανισμό έως το σωστό σχεδιασμό αυθεντικοποίησης και εξουσιοδότησης χρηστών όσον αφορά την δομή του οργανισμού και τέλος την χρήση τεχνολογιών VPN, αντιικών, συστημάτων IDS, IPS και ισχυρή κρυπτογράφηση από άκρο σε άκρο της επικοινωνίας.

4 Τελικά Συμπεράσματα

Ο στόχος της κλιματικής ουδετερότητας της Ευρώπης έως το 2050, προκειμένου να αποφευχθεί η περαιτέρω άνοδος της θερμοκρασίας, λόγω του φαινομένου του θερμοκηπίου μέσω των ρύπων που εκλύονται, δύναται να επιτευχθεί έπειτα από παρεμβάσεις στους οικονομικούς τομείς που την καθορίζουν και υιοθετώντας την εφαρμογή των Τεχνολογιών Πληροφορικής κι Επικοινωνιών (ICT). Εάν δεν μετριαστεί το φαινόμενο της Κλιματικής Κρίσης, σε σενάριο αύξησης της θερμοκρασίας κατά 3 βαθμούς Κελσίου σε σύγκριση με τα προβιομηχανικά επίπεδα, σύμφωνα με το Joint Research Center της Ευρωπαϊκής Ένωσης, πέραν των συγκλονιστικών επιπτώσεων στο περιβάλλον και την υγεία, εκτιμάται πως η ευρωπαϊκή οικονομία θα ζημειωθεί κατά 190 δις €.

Συν τοις άλλοις, το Παγκόσμιο Οικονομικό Φόρουμ αναδεικνύει πως τα τελευταία 30 χρόνια, για κάθε 1 δολάριο που επενδύεται στις ψηφιακές τεχνολογίες, η αύξηση του ΑΕΠ είναι 20 δολάρια, ενώ για τις μη ψηφιακές επενδύσεις είναι μόλις 3 δολάρια. Βάσει των ίδιων υπολογισμών, το 25% του παγκόσμιου ΑΕΠ θα προέρχεται από την ψηφιακή τεχνολογία μέχρι το 2025.[97]

Επιπλέον, κατά την περίοδο του κορωνοϊού βιώσαμε έναν ραγδαίο ψηφιακό μετασχηματισμό, ο οποίος ούτως ή άλλως είναι άρρηκτα συνδεδεμένος με την πράσινη μετάβαση της Ευρωπαϊκής Ένωσης. Με τον όρο ψηφιακό μετασχηματισμό εννοούμε την διείσδυση των ψηφιακών τεχνολογιών στις διαδικασίες του ιδιωτικού και δημοσίου τομέα. Σε αυτές τις ψηφιακές τεχνολογίες συγκαταλέγονται τεχνολογίες αιχμής της Πληροφορικής και των Επικοινωνιών, όπως οι ψηφιακές πλατφόρμες, επί παραδείγματι η τηλεκπαίδευση κατά τη πανδημία και η δημιουργία του gov.gr, το Διαδίκτυο των Πραγμάτων, η τεχνολογία Blockchain, το υπολογιστικό νέφος και η Τεχνητή Νοημοσύνη. Ωστόσο, η ταχεία υιοθέτηση αυτών των τεχνολογιών και ειδικά όταν το 42% των πολιτών της Ε.Ε. παρουσιάζει ελλείψεις σε βασικές ψηφιακές δεξιότητες ενδέχεται να ελλοχεύει κινδύνους. Η λήψη και τήρηση μέτρων ασφαλείας σε αυτές τις κρίσιμες υποδομές πληροφοριακών συστημάτων και γενικότερα στον κυβερνοχώρο επιτυγχάνεται με την Κυβερνοασφάλεια. Με το πρόγραμμα Ψηφιακή Ευρώπη που ενέκρινε το Ευρωπαϊκό Κοινοβούλιο τον Απρίλιο του 2021 επενδύονται 1,6 δις € στη Κυβερνοασφάλεια, 577 εκατομμύρια € στις εξελιγμένες ψηφιακές δεξιότητες και 1,1 δις € στη διεύρυνση της χρήσης των ψηφιακών τεχνολογιών σε ολόκληρη την οικονομία και την κοινωνία της Ε.Ε.[98]

Στην παρούσα διπλωματική εργασία εξετάστηκε το ζήτημα της εφαρμογής της Κυβερνοασφάλειας στους κυριότερους τομείς που έχουν κομβικό ρόλο στην αντιμετώπιση της Κλιματικής Κρίσης, δηλαδή στην Ψηφιακή Γεωργία, στη Μεταφορά και Αποθήκευση προϊόντων (Logistics) και στην Ενέργεια και στις Έξυπνες Πόλεις.

Στο πρώτο κεφάλαιο αναδείχθηκε η σημασία της Κυβερνοασφάλειας στη Γεωργία Ακριβείας πραγματοποιώντας βιβλιομετρική ανάλυση στην επιστημονική βάση δημοσιεύσεων scopus.comμε το πρόγραμμα VOSViewer. Με αυτό το εργαλείο παρουσιάστηκαν οι τάσεις της έρευνας με γνώμονα τους όρους “agriculture” και

[97] Πηγή: https://masters.ds.unipi.gr/MSc_Climate_ICT/category/msc-climate-ict-1/

[98] Πηγή: https://www.europarl.europa.eu/news/el/headlines/society/20210414STO02010/diamorfosi-psifiakou-metaschimatismou-epexigisi-tis-stratigikis-tis-ee

“cybersecurity” επιστρέφοντας ως επικρατέστερους όρους τα “agriculture robots”, το “network security”, το “internet security” και τα “smart agricultures”. Στο πεδίο του χρόνου από τον Ιούνιο του 2020 και μετά, οι πιο πρόσφατοι και κυριότεροι όροι που αναδείχθηκαν στην έρευνα είναι οι “security threats”, η “industry 4.0”, το “intrusion detection”, το “food supply” και το “smart farming”.Στη συνέχεια, παρουσιάστηκε η ανατομία των κυβερνοεπιθέσεων, ενώ συν τοις άλλοις αναλύθηκαν ενδελεχώς οι επιθέσεις τύπου Advanced Persistent Threat σε αγροκτήματα που εφαρμόζουν τεχνολογίες ακριβείας. Τέλος, προτάθηκαν αντίμετρα όπως η θωράκιση των IoT συσκευών, η χρήση IoT Gateway, ενώ κρίθηκε αναγκαία η υιοθέτηση της τεχνολογίας Blockchain που αναλύθηκε ενδελεχώς στο επόμενο κεφάλαιο.

Εν συνεχεία, στο δεύτερο κεφάλαιο παρουσιάστηκαν εφαρμογές του πρωτοκόλλου Κυβερνοασφάλειας του μέλλοντος του Blockchain στον τομέα των Μεταφορών και της Αποθήκευσης προϊόντων (Logistics). Με τη χρήση του VOSViewer κι εδώ βάσει της αναζήτησης στην scopus.com των όρων “blockchain” και “logistics” αναδείχθηκαν βιβλιομετρικά οι ισχυρότεροι όροι στο συγκεκριμένο επιστημονικό πεδίο με κυριότερους τη “supply chain”, τη “blockchain technology”, το “internet of things” κι εδώ όπως και στο προηγούμενο κεφάλαιο, και τα “smart contracts” που αποτελούν συστατικό του πρωτοκόλλου Blockchain. Ακολούθως, παρουσιάστηκαν ο ορισμός της Blockchain, παραδείγματα της σε υπηρεσίες Logistics και στην εφοδιαστική αλυσίδα στη βιομηχανία τροφίμων. Μετέπειτα, παρουσιάστηκε ενδελεχώς το σύστημα τεχνολογίας Blockchain FoodTrust της IBM και τις λύσεις που προσφέρει βάσει επιμέρους ερευνών όσον αφορά την αποτελεσματικότητα της Εφοδιαστικής Αλυσίδας, το Brand Trust, την Ασφάλεια και φρεσκάδα των τροφίμων, τη βιωσιμότητα και την αντιμετώπιση των προβληματικών τροφίμων αλλά και του φαινομένου κατασπατάλησής τους. Η έρευνα καταλήγει στην αναγκαιότητα ανάπτυξης της τεχνολογίας Blockchain λόγω της διαφάνειας και ιχνηλασιμότητας που προσφέρει, μαζί με τις τεχνολογίες IoT και 5G - 6G εφόσον όλες είναι άρρηκτα συνδεδεμένες για να επιφέρουν με ακρίβεια και ταχύτητα τα καλύτερα αποτελέσματα.

Τέλος, στο τρίτο κεφάλαιο όσον αφορά τον χώρο της Ενέργειας και των Έξυπνων Πόλεων του μέλλοντος, διεξήχθη έρευνα στην Κυβερνοασφάλεια για τα επερχόμενα Έξυπνα Δίκτυα Παροχής Ηλεκτρικού Ρεύματος (Smart Grids). Παρουσιάστηκαν οι ορισμοί, τα χαρακτηριστικά, τα δομικά και οικονομικά στοιχεία αλλά και οι προκλήσεις των Έξυπνων Δικτύων καθώς και η σύγκρισή τους με τα παραδοσιακά δίκτυα παροχής ηλεκτρισμού. Έπειτα, αναδείχθηκαν το υφιστάμενο νομικό πλαίσιο της Ευρωπαϊκής Ένωσης που τα αφορά, καθώς και οι στόχοι και οι πολιτικές Κυβερνοασφάλειας και το κόστος και η κατηγοριοποίηση των Κυβερνοεπιθέσεων. Παρατέθηκαν πιθανές βασικές επιθέσεις στα Έξυπνα Δίκτυα όπως το Ηλεκτρονικό Ψάρεμα (Phishing), η Άρνηση της Υπηρεσίας (Denial of Service), ο Διαμοιρασμός Κακόβουλου Λογισμικού (Malware Spreading), η Υποκλοπή και ανάλυση της κίνησης της πληροφορίας (Eavesdropping and traffic analysis). Μελετήθηκαν οι διάσημες Κυβερνοεπιθέσεις σε κρίσιμες υποδομές παροχής ενέργειας όπως η BlackEnergy, το Stuxnet και το WannaCry και προτάθηκαν μέτρα για τη θωράκιση έναντι αυτών κι αντιμετώπισή τους. Σε αυτά τα μέτρα συγκαταλέγονται η τήρηση της πολιτικής ασφαλείας για ισχυρούς κωδικούς, της κρυπτογράφησης κι αυθεντικοποίησης των δεδομένων και παράλληλα προτάθηκε η προστασία απειλών με Αντιικά, IPS, IDS και χρήση τεχνολογίας VPN.

Η παρούσα μελέτη ανέδειξε τη σπουδαιότητα της Κυβερνοασφάλειας σε κάθε νέα εφαρμογή των νέων τεχνολογιών στους τομείς που καθορίζουν την Κλιματική

Κρίση. Με την ραγδαία ταχύτητα του ψηφιακού μετασχηματισμού που βιώσαμε κατά τη περίοδο του κορωνοϊού και την ανάδειξη της Τεχνητής Νοημοσύνης που θα κατέχει σημαντικό ρόλο στην αυτοματοποίηση των διαδικασιών και λήψη αποφάσεων δε πρέπει να ξεχνάμε πως στο επίκεντρο όλων οφείλει να είναι ο άνθρωπος και η ευημερία του πάντα σε συνάρτηση με το σεβασμό στο περιβάλλον, στα οικοσυστήματα και στον πλανήτη επιδιώκοντας διαρκώς τη βιωσιμότητα και χωρίς τη παράδοση όλων αυτών στο βωμό του κέρδους.

4.1 Προτάσεις για περαιτέρω έρευνα

Πέραν των ζητημάτων που εξετάστηκαν, με έναυσμα την παρούσα διπλωματική εργασία, θέματα για επιπλέον έρευνα είτε σε γειτνιάζουσα, είτε σε πιο εξειδικευμένη περιοχή στους τομείς που μελετήθηκαν, θα μπορούσαν να είναι τα κάτωθι:

1) Σχεδιασμός και υλοποίηση δικτύου αισθητήρων σε αληθινό χωράφι με λήψη μέτρων κυβερνοασφάλειας: Εφαρμογή Firewall – IoT Gateway σε σύστημα Ακριβούς Γεωργίας.
2) Η Κυβερνοασφάλεια στα Αυτόνομα Οχήματα και στη Ναυτιλία: Μελέτη και υλοποίηση δικτύου ασφαλών τηλεπικοινωνιών. Πρωτόκολλα επικοινωνιών κι αποτροπή επιθέσεων. Ο ρόλος της τεχνητής νοημοσύνης στην ανίχνευση απειλών στα Logistics.
3) Υλοποίηση μεθόδων Κυβερνοασφάλειας για το Έξυπνο Σπίτι. Δημιουργία ξεχωριστών δικτύων για τις IoT συσκευές και προστασία τους. Αποτροπή σεναρίων κυβερνοεπιθέσεων με Firewall – IoT Gateway. Penetration test σε δημιουργηθείσα μικρή υποδομή δικτύου ψηφιακών συσκευών.

Βιβλιογραφία

1. Angyalos, Zsanett, Szilvia Botos, and Szilagyi Robert. "The Importance of Cybersecurity in Modern Agriculture." Journal of Agricultural Informatics 12 (Ιούλιος 15, 2021). https://doi.org/10.17700/jai.2021.12.2.604.
2. Bhat, Showkat Ahmad, Nen-Fu Huang, Ishfaq Bashir Sofi, and Muhammad Sultan. "Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability." Agriculture 12, no. 1 (Ιανουάριος 2022): 40. https://doi.org/10.3390/agriculture12010040.
3. "Bibliometrics." Στη Wikipedia, Ιούνιος 14, 2022. https://en.wikipedia.org/w/index.php?title=Bibliometrics&oldid=1093153031.
4. FBI. "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies.", τελ. ανάκτηση 19/07/2022 από https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.
5. ec.europa.eu ."Farmers and the Agricultural Labour Force - Statistics.", τελ. ανάκτηση 19/07/2022 από https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Farmers_and_the_agricultural_labour_force_-_statistics.
6. Gupta, Maanak, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. "Security and Privacy in Smart Farming: Challenges and Opportunities." IEEE Access PP (Φεβρουάριος 19, 2020): 1–1. https://doi.org/10.1109/ACCESS.2020.2975142.
7. Industrial Software. "Industrial Cyber Security Guide | ABB.", τελ. ανάκτηση 18/07/2022 από https://new.abb.com/industrial-software/industrial-cyber-security-guide.
8. "Low-Power Wide-Area Network." Στη Wikipedia, Μάρτιος 16, 2022. https://en.wikipedia.org/w/index.php?title=Low-power_wide-area_network&oldid=1077542034.
9. "MikroTik." , τελ. ανάκτηση 19/07/2022 από https://mikrotik.com/.
10. Pappula, Praveen, Mohammed Shaik, Sampath Kumar, and Tanupriya Choudhury. "Smart Farming: Securing Farmers Using Block Chain Technology and IOT," 225–38, 2021. https://doi.org/10.1007/978-3-030-65691-1_15.
11. "Precision Agriculture." Στη Wikipedia, Ιούλιος 1, 2022. https://en.wikipedia.org/w/index.php?title=Precision_agriculture&oldid=1095898381.
12. Ritchie, Hannah, and Max Roser. "Land Use." Our World in Data, Νοέμβριος 13, 2013. https://ourworldindata.org/land-use.
13. Roser, Max. "Future Population Growth." Our World in Data, Μάιος 9, 2013. https://ourworldindata.org/future-population-growth.
14. "Side-Channel Attack." Στη Wikipedia, Ιούνιος 7, 2022. https://en.wikipedia.org/w/index.php?title=Side-channel_attack&oldid=1092051943.
15. Smith, Zhanna Malekos, Eugenia Lostri, and James A Lewis. "The Hidden Costs of Cybercrime," n.d., 38.
16. Sontowski, S., M. Gupta, S.S. Laya Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi, and R. Sandhu. "Cyber Attacks on Smart Farming Infrastructure," 135–43, 2020. https://doi.org/10.1109/CIC50333.2020.00025.

17. VOSviewer. “VOSviewer - Visualizing Scientific Landscapes.” τελ. ανάκτηση 10/07/2022 από https://www.vosviewer.com//.
18. www.kaspersky.com. “What Is an Advanced Persistent Threat (APT)?,”, τελ. ανάκτηση 08/01/2022 από https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.
19. Learning Center. “What Is APT (Advanced Persistent Threat) | APT Security | Imperva.”, τελ. ανάκτηση 18/07/2022 από https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.
20. Cisco. “What Is Cybersecurity?”,τελ. ανάκτηση 18/07/2022 από https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.
21. Yazdinejad, Abbas, Behrouz Zolfaghari, Amin Azmoodeh, Ali Dehghantanha, Hadis Karimipour, Evan Fraser, Arthur Green, Conor Russell, and Emily Duncan. “A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures.” Applied Sciences 11 (Αύγουστος 16, 2021): 7518. https://doi.org/10.3390/app11167518.
22. Yi, Shanhe, Zhengrui Qin, and Qun Li. “Security and Privacy Issues of Fog Computing: A Survey,” 685–95, 2015. https://doi.org/10.1007/978-3-319-21837-3_67.
23. gaiasense - Ευφυής γεωργία. “Γίνετε πρωτοπόροι της ευφυούς γεωργίας στην Ελλάδα | gaiasense.”,τελ. ανάκτηση 18/07/2022 από https://www.gaiasense.gr/gaiasense.
24. www.aimspress.com. “Cybersecurity in smart grids, challenges and solutions”, τελ. ανάκτηση 09/02/2022 από https://www.aimspress.com/article/id/5ffd82bcba35de34e6cde4bd
25. www.nist.gov. “Guidelines for smart grid cybersecurity.”, τελ. ανάκτηση 08/01/2022 από https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity
26. nvlpubs.nist.gov. “Guidelines for smart grid cybersecurity.”, τελ. ανάκτηση 09/02/2022 από https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
27. pureadmin.qub.ac.uk. “Threat Analysis of BlackEnergy Malware for Synchrophasor based Real time Control and Monitoring in Smart Grid”, τελ. ανάκτηση 11/02/2022 από https://pureadmin.qub.ac.uk/ws/portalfiles/portal/86558342/Threat_Analysis_of_BlackEnergy_Malware_for_Synchrophasor_based_Real_time_Control_and_Monitoring_in_Smart_Grid.pdf
28. www.techtarget.com. “Sandbox (software testing and security).”, τελ. ανάκτηση 17/02/2022 από https://www.techtarget.com/searchsecurity/definition/sandbox
29. www.iperiusbackup.net. “Virtual machines and sandboxes. How to use them within VMware Workstation Player.”, τελ. ανάκτηση 09/02/2022 από https://www.iperiusbackup.net/en/virtual-machines-and-sandboxes-to-use-them-within-vmware-workstation-player/
30. generatepasswords.org. “How to Calculate Password Entropy,” τελ. ανάκτηση 08/01/2022 από https://generatepasswords.org/how-to-calculate-entropy/
31. www.ebcg.com. “ Blackenergy or how to hack an energy provider.”, τελ. ανάκτηση 09/02/2022 από https://www.ebcg.com/blackenergy-or-how-to-hack-an-energy-provider/

32. citeseerx.ist.psu.edu. “A survey on the communication architectures in smart grid.”, τελ. ανάκτηση 20/01/2022 από https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.713.303&rep=rep1&type=pdf
33. www.researchgate.net. “Analysis of cyber-attacks on smart grid applications.”, τελ. ανάκτηση 09/02/2022 από https://www.researchgate.net/publication/331418396_Analysis_of_cyber-attacks_on_smart_grid_applications
34. www.kaspersky.com. “What are the different types of malware?,”, τελ. ανάκτηση 04/01/2022 από https://www.kaspersky.com/resource-center/threats/types-of-malware
35. www.trendmicro.com. “Spear phishing.”, τελ. ανάκτηση 09/02/2022 από https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing
36. “SCADA.” Στη Wikipedia, Φεβρουαρίου 9, 2022 https://el.wikipedia.org/wiki/SCADA
37. www.telstarinc.com. “How SCADA, HMI, and PLC Work Together.”, τελ. ανάκτηση 09/02/2022 από https://www.telstarinc.com/blog/how-scada-hmi-and-plc-work-together/
38. smartgrid.epri.com. “Cyber Security for Power Delivery and Utilization”, τελ. ανάκτηση 21/01/2022 από https://smartgrid.epri.com/
39. ico.org.uk. “What types of encryption are there?”, τελ. ανάκτηση 09/02/2022 από https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-types-of-encryption-are-there/
40. Σταύρος Γριμάνης, ΔΕΔΔΗΕ: Πώς θα τρέξει το megaproject των «έξυπνων μετρητών», Newmoney, 2022
41. Χρυσόγελος Ν.,Ο Ενεργειακός Τομέας στην Ελλάδα . Η πράσινη οπτική , Μάιος 2015
42. Baseem Khan, EsayasGidey, HabtamuGetachew, Hassan HaesAlhelou, Managing the generation and demand inside the smart-grid structure, Editor(s): John R. Vacca, Solving Urban Infrastructure Problems Using Smart, City Technologies, Elsevier, 2021.
43. Cambell R, The Smart Grid: Status and Outlook, Απρίλιος 2018.
44. Covrig Laura, G. F., Smart Grids and Beyond: An EU research. Luxembourg: Publications Office of the European Union, 2011.
45. C. Li et al., "Grid architecture for future distribution system — A cyber-physical system perspective," IECON 2017 - 43rd Annual Conference of the IEEE Industrial ElectrSeventh framework programme of the European Community for research and technological development including demonstration activities(FP7). Ανάκτηση από European Commission: https://cordis.europa.eu/programme/id/FP7, 2015.
46. David Lineweber, S. M.,The Cost of Power Disturbances to. Wisconsin: EPRI. 2001.
47. Dileep G, A survey on smart grid technologies and applications, Renew Energ 146: 2589–2625, 2020.
48. Dimitrios Chaniotis, Laurent Schmitt, Connecting Europe: Electricity, Entso-e, 2018.
49. Divatia A., A Blueprint For Cybersecurity Investment In 2022, Forbes, 2021.
50. European Commission, European Smart Grids Technology Platform: www.smartgrids.eu/

51. Khan R, Maynard P, McLaughlin K, et al. ,Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, 53-63, 2016
52. Larik, Raja Masood, Technologies Used in Smart Grid to Implement Power Distribution System, Journal of Electrical Engineering, (2018)
53. LiuJ, XiaoY, LiS, Cyber security and privacy issues in smart grids. IEEE CommunSurvTut 14: 981–997, (2012)
54. Magill, J., Experts Say Cyberattacks Likely To Result In Blackouts In U.S. Forbes, (2021)
55. Maglaras LA, Kim KH, Janicke H, Cyber security of critical infrastructures. Ict Express 4: 42–45, (2018)
56. Miller J , The Smart Grid – Benefits and Challenges ,EEI Annual Convention – Toronto, Modern Grid Strategy Team Ιούνιος 16, (2008)
57. An update on food fraud. (2020, Ιανουάριος 31). Food Safety Net Services. https://fsns.com/an-update-on-food-fraud/
58. Blockchain in Logistics. (2020). PwC. https://www.pwc.de/de/strategie-organisation-prozesse-systeme/blockchain-in-logistics.pdf
59. connect.comptia.org.“Blockchain terminology—A glossary for beginners | blockchain | comptia. (n.d.) ”, Default. , τελ. ανάκτηση 23/06/2022 από http://connect.comptia.org/content/articles/blockchain-terminology
60. www.juniperresearch.com.“Blockchain to save the food industry $31 billion by 2024, driven by iot partnerships. (n.d.) ”,τελ. ανάκτηση 23/06/2022 από https://www.juniperresearch.com/press/press-releases/blockchain-to-save-the-food-industry-31-billion
61. Calculating the cost of food miles. (2019, Αύγουστος 19). Babylon Micro-Farms. https://babylonmicrofarms.com/calculating-the-cost-of-food-miles/
62. Consumer research on sustainable eating and food waste. (2019, Σεπτέμβρης 17). Food Insight. https://foodinsight.org/consumers-insights-future-of-food-sustainability-food-waste/
63. www.fleetboard.info.“Fleetboard: Blockchain ecosystem. (n.d.) ”, τελ. ανάκτηση 23/06/2022 από https://www.fleetboard.info/news/blockchain-ecosystem/#/
64. www.fao.org .“Food loss and waste database. (n.d.). Food and Agriculture Organization of the United Nations”, τελ. ανάκτηση 23/06/2022 από http://www.fao.org/platform-food-loss-waste/flw-data/en/
65. www.food-safety.com .“Food safety. (n.d.) ”, τελ. ανάκτηση 23/06/2022 από https://www.food-safety.com/gdpr-policy?url=https%3A%2F%2Fwww.food-safety.com%2Farticles%2F6487-a-look-back-at-2019-food-recalls
66. foodnavigator-usa.com. “ (n.d.-a). Deloitte: Fresh food spending is on the rise, but the store perimeter is still underperforming. Foodnavigator-Usa.Com”, τελ. ανάκτηση 23/06/2022 από https://www.foodnavigator-usa.com/Article/2019/11/13/Deloitte-report-Consumers-fresh-food-spending-on-the-rise
67. foodnavigator-usa.com. “ (n.d.-b). Nielsen: Which sustainability attributes matter most to consumers? Foodnavigator-Usa.Com”,τελ. ανάκτηση 23/06/2022 από https://www.foodnavigator-usa.com/Article/2019/12/03/Nielsen-Which-sustainability-attributes-matter-most-to-consumers
68. Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat?ECONSTOR; ECONSTOR. https://www.econstor.eu/bitstream/10419/209299/1/hicl-2017-23-003.pdf

69. thegemba.com .“How Walmart used blockchain to increase supply chain transparency. (n.d.) ”, τελ. ανάκτηση 23/06/2022 από https://thegemba.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency
70. IBM. (2015, October 1). 7 benefits of ibm food trust. IBM. https://www.ibm.com/blockchain/resources/7-benefits-ibm-food-trust
71. www.ibm.com .“IBM supply chain intelligence suite—Food trust. (n.d.) ”, τελ. ανάκτηση 23/06/2022 από https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust
72. corporate.walmart.com .“In wake of romaine e. Coli scare, walmart deploys blockchain to track leafy greens. (n.d.). Corporate - US”, τελ. ανάκτηση 23/06/2022 από https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens
73. newmoney, Ε. για την Ο. |. (2022, May 23). EBRD: Η Ελλάδα μπορεί να ωφεληθεί από την αποπαγκοσμιοποίηση. Ειδήσεις για την Οικονομία | newmoney. https://www.newmoney.gr/roh/palmos-oikonomias/oikonomia/ebrd-i-ellada-bori-na-ofelithi-apo-tin-apopagkosmiopiisi/
74. theanalyticalscientist.com.“Piracy in the pantry. (n.d.) ”. The Analytical Scientist”, τελ. ανάκτηση 23/06/2022 από https://theanalyticalscientist.com/fields-applications/piracy-in-the-pantry
75. www.snackandbakery.com.“Snack food & wholesale bakery. (n.d.) ”,τελ. ανάκτηση 23/06/2022 από https://www.snackandbakery.com/gdpr-policy?url=https%3A%2F%2Fwww.snackandbakery.com%2Farticles%2F92105-evaluating-the-real-costs-of-a-food-product-recall
76. www.fao.org .“Sustainable Development Goals. (n.d.) ”, τελ. ανάκτηση 23/06/2022 από https://www.fao.org/sustainable-development-goals/indicators/1231/en
77. sustainablefoodtrust.org . “Sustainable food trust—True cost accounting. (n.d.). Sustainable Food Trust”, τελ. ανάκτηση 23/06/2022 από https://sustainablefoodtrust.org/our-work/true-cost-accounting/
78. Tackling the 1. 6-billion-ton food loss and waste crisis. (2020, Ιούλιος 18). BCG Global. https://www.bcg.com/publications/2018/tackling-1.6-billion-ton-food-loss-and-waste-crisis
79. www.logmore.com . “The challenges of fresh produce logistics – logmore blog. (n.d.) ”, τελ. ανάκτηση 23/06/2022 από https://www.logmore.com/post/the-challenges-of-fresh-produce-logistics
80. The cost of food spoilage | cargo data corp. (2017, Δεκέμβριος 15). Cargo Data. https://cargodatacorp.com/cost-food-spoilage/
81. www2.deloitte.com . “The future of fresh. (n.d.). Deloitte Insights. ”, τελ. ανάκτηση 23/06/2022 από https://www2.deloitte.com/us/en/insights/industry/retail-distribution/future-of-fresh-food-sales/pandemic-consumer-behavior-grocery-shopping.html
82. www.lrqa.com .“The modern uk food shopper revealed. (n.d.). LRQA”, τελ. ανάκτηση 23/06/2022 από https://www.lrqa.com/en-gb/resources/2019-uk-food-survey/
83. www.tracegains.com . “The real cost of food fraud. (n.d.) ” , τελ. ανάκτηση 23/06/2022 από https://www.tracegains.com/blog/the-real-cost-of-food-fraud

84. US EPA, O. (2016, Απρίλιος 14). United states 2030 food loss and waste reduction goal [Overviews and Factsheets]. https://www.epa.gov/sustainable-management-food/united-states-2030-food-loss-and-waste-reduction-goal
85. "VOSviewer—Visualizing scientific landscapes. (n.d.). VOSviewer", τελ. ανάκτηση 23/06/2022 από https://www.vosviewer.com//
86. archive-yaleglobal.yale.edu . "World population: 2020 overview | yaleglobal online. (n.d.) " , τελ. ανάκτηση 23/06/2022 από https://archive-yaleglobal.yale.edu/content/world-population-2020-overview
87. www.pcsteps.gr. "Τι Είναι η Blockchain: Όλη η Αλήθεια για τις Αμέτρητες Εφαρμογές Της | PCsteps.gr. (n.d.) " , τελ. ανάκτηση 23/06/2022 από https://www.pcsteps.gr/214154-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7-blockchain-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82/